PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-032037

(43)Date of publication of application : 02.02.1999

(51)Int.Cl. H04L 9/32
G06F 9/06
G06F 15/00
G09C 1/00

(21)Application number : 09-188801

(22)Date of filing : 14.07.1997

(71)Applicant : FUJI XEROX CO LTD

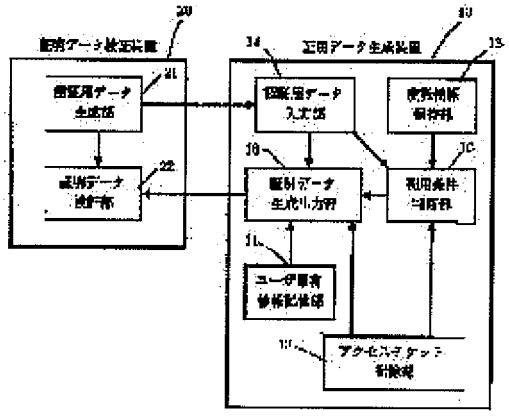
(72)Inventor : NAKAGAKI JUHEI
SHIN YOSHIHIRO

(54) CERTIFICATION DATA GENERATING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To pre-pay access qualification to purchase or rent without imposing any surplus load on a certification data generating device side.

SOLUTION: A pre-paid purchase ticket T2 is stored in an access ticket storing part 13. Next, (T1', n2) is inputted to a certification data-imputting part 14. A use condition judging part 15 extracts a corresponding access ticket (t2, L2, n2), checks whether or not a use condition L2 is fulfilled, and reduces frequency information V, when the use condition is fulfilled. A certification data generating and outputting part 16 calculates certification data R by using auxiliary certification decision (t)2 and the use condition L2 extracted by the use condition decision part 15 and (du) read from a user specific information storing part 11, and outputs T1. A user performs access to a program in a purchase state or a rent state by using the T1.



LEGAL STATUS

[Date of request for examination] 25.10.2001

[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3641909
[Date of registration]	04.02.2005
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] In the certification data generation equipment which is generated in order to attest a user's access rating, and generates the certification data which have justification verified A data input means for authentication to input the data for authentication, and a user proper information storage means to memorize a user's proper information, The auxiliary information for certification which performed and generated predetermined count to a user's proper information, the description information on access rating authentication, and the use condition information that described the access condition, An auxiliary information set storage means for certification to memorize the auxiliary information set for certification containing a group with use condition information, The auxiliary information set for certification corresponding to the inputted data for authentication is taken out from the above-mentioned auxiliary information set storage means for certification. The above-mentioned picking when it is judged as continuation in the use conditional-judgment means and the above-mentioned use conditional-judgment means of judging whether subsequent processings being continued, according to the use condition information on the taken-out auxiliary information set for certification The above-mentioned picking The taken-out auxiliary information set for certification, and the data for authentication inputted from the above-mentioned data input means for authentication, Perform predetermined count to the above-mentioned user's proper information memorized by the above-mentioned user proper information storage means, and it has a certification data generation output means to generate and output certification data. From the above-mentioned data input means for authentication, the auxiliary information set for encryption certification which enciphered the 1st auxiliary information set for certification with the encryption key in a code function is inputted. The above-mentioned use conditional-judgment means The 2nd auxiliary information set for certification corresponding to the inputted auxiliary information set for encryption certification is taken out from the above-mentioned auxiliary information set storage means for certification. After performing predetermined processing according to the use condition information on the 2nd auxiliary information set for certification taken [above-mentioned] out picking, it judges whether subsequent processings are continued. The above-mentioned certification data generation output means Certification data generation equipment characterized by outputting the 1st auxiliary information set for certification which is the result of decrypting the above-mentioned auxiliary information set for encryption certification by performing the above-mentioned processing.
[Claim 2] Certification data generation equipment according to claim 1 currently held in a defense means to close at least that the above-mentioned user proper information storage means, the above-mentioned use conditional-judgment means, and the above-mentioned certification data generation output means observe internal data and processing procedure from the outside if .
[Claim 3] It has a frequency information maintenance means to hold electronic frequency information furthermore. To the above-mentioned use condition information The number of availabilities which should be paid when it uses is included. The above-mentioned use conditional-judgment means The electronic frequency information currently held at the above-mentioned frequency information

maintenance means is compared with the number of availabilities contained in the above-mentioned use condition information. The frequency for several availability minutes contained in the above-mentioned use condition information from the electronic frequency information currently held for the above-mentioned frequency information maintenance means only at the time more than the number of availabilities by which the electronic frequency information currently held at the above-mentioned frequency information maintenance means is included in use condition information is reduced. Certification data generation equipment according to claim 1 or 2 which makes judgment of continuing subsequent processings.

[Claim 4] The number of availabilities which the number of availabilities contained in the 1st use condition information contained in the auxiliary information set for certification of the above 1st is zero frequency, and is contained in the 2nd use condition information contained in the auxiliary information set for certification of the above 2nd is certification data generation equipment according to claim 3 characterized by being except zero.

[Claim 5] It is certification data generation equipment according to claim 1, 2, 3, or 4 which makes judgment of continuing subsequent processings only when it has the clock in which time of day is furthermore shown, and expiration date information is further indicated by the 1st use condition information contained in the auxiliary information set for certification of the above 1st, the above-mentioned use conditional-judgment means compares the above-mentioned time of day and the above-mentioned expiration date information with it and this time of day is within an expiration date.

[Claim 6] Certification data generation equipment according to claim 1, 2, 3, 4, or 5 constituted at least as a small arithmetic unit which means other than the above-mentioned auxiliary information set storage means for certification can carry.

[Claim 7] In the access rating authentication equipment which attests the above-mentioned user's access rating by verifying the justification of the certification data generated in order to prove a user's access rating The 1st storage means which memorizes the data for authentication, and the 2nd storage means which memorizes a user's proper information, The 3rd storage means which memorizes the auxiliary information for encryption certification which enciphered and generated the 1st auxiliary information for certification which performed and generated predetermined count to the above-mentioned user's proper information, and the description information on access rating authentication, As opposed to the above-mentioned user's proper information, the decode key of the above-mentioned encryption, and the use condition information that described the access condition The 4th storage means which memorizes the 2nd auxiliary information set for certification which consists of the 2nd auxiliary information for certification which performed and generated predetermined count, and the above-mentioned use condition information, When it judges that a means to judge whether predetermined processing is continued according to the above-mentioned use condition information included in the auxiliary information set for certification of the above 2nd memorized by the storage means of the above 4th, and the above-mentioned predetermined processing are continued The above-mentioned auxiliary information for encryption certification memorized by the storage means of the above 3rd, A means to perform predetermined count to the above-mentioned user's proper information memorized by the storage means of the above 2nd, and the auxiliary information set for certification of the above 2nd memorized by the storage means of the above 4th, and to restore the auxiliary information for certification on the above 1st, The above-mentioned data for authentication memorized by the storage means of the above 1st, and the above-mentioned user's proper information memorized by the storage means of the above 2nd, Access rating authentication equipment characterized by having a means to perform predetermined count to the auxiliary information for authentication on the restored above 1st, and to generate certification data, and a means to verify the generated above-mentioned certification data.

[Claim 8] In the access rating authentication equipment which attests the above-mentioned user's access rating by verifying the justification of the certification data generated in order to prove a user's access rating The 1st storage means which memorizes the data for authentication, and the 2nd storage means which memorizes a user's proper information, The 1st auxiliary information for certification which

performed and generated predetermined count to the above-mentioned user's proper information, the description information on access rating authentication, and the 1st use condition information that described the access condition, The 3rd storage means which memorizes the auxiliary information set for encryption certification which enciphered and generated the 1st auxiliary information set for certification which consists of use condition information on the above 1st, As opposed to the above-mentioned user's proper information, the decode key of the above-mentioned encryption, and the 2nd use condition information that described the access condition The 4th storage means which memorizes the 2nd auxiliary information set for certification which consists of the 2nd auxiliary information for certification which performed and generated predetermined count, and use condition information on the above 2nd, A means to judge whether the 1st processing is continued according to the use condition information on the above 2nd included in the auxiliary information set for certification of the above 2nd memorized by the storage means of the above 4th, and when it judges that the 1st above-mentioned processing is continued The above-mentioned auxiliary information set for encryption certification memorized by the storage means of the above 3rd, A means to perform predetermined count to the above-mentioned user's proper information memorized by the storage means of the above 2nd, and the auxiliary information set for certification of the above 2nd memorized by the storage means of the above 4th, and to restore the auxiliary information set for certification of the above 1st, A means to judge whether the 2nd processing is continued according to the use condition information on the above 1st included in the auxiliary information set for certification of the restored above 1st, and when it judges that the 2nd above-mentioned processing is continued The above-mentioned data for authentication memorized by the storage means of the above 1st, and the above-mentioned user's proper information memorized by the storage means of the above 2nd, Access rating authentication equipment characterized by having a means to perform predetermined count to the auxiliary information set for certification of the restored above 1st, and to generate certification data, and a means to verify the generated above-mentioned certification data.

[Claim 9] In the access rating authentication approach which attests the above-mentioned user's access rating by verifying the justification of the certification data generated in order to prove a user's access rating The 1st step which memorizes the data for authentication, and the 2nd storage step which memorizes a user's proper information, The 1st auxiliary information for certification which performed and generated predetermined count to the above-mentioned user's proper information, the description information on access rating authentication, and the 1st use condition information that described the access condition, The 3rd step which memorizes the auxiliary information set for encryption certification which enciphered and generated the 1st auxiliary information set for certification which consists of use condition information on the above 1st, As opposed to the above-mentioned user's proper information, the decode key of the above-mentioned encryption, and the 2nd use condition information that described the access condition The 4th storage step which memorizes the 2nd auxiliary information set for certification which consists of the 2nd auxiliary information for certification which performed and generated predetermined count, and use condition information on the above 2nd, The step which judges whether the 1st processing is continued according to the use condition information on the above 2nd included in the auxiliary information set for certification of the above 2nd memorized at the storage step of the above 4th, and when it judges that the 1st above-mentioned processing is continued The above-mentioned auxiliary information set for encryption certification memorized at the storage step of the above 3rd, The step which performs predetermined count to the above-mentioned user's proper information memorized at the storage step of the above 1st, and the auxiliary information set for certification of the above 2nd memorized at the storage step of the above 4th, and restores the auxiliary information set for certification of the above 1st, The step which judges whether the 2nd processing is continued according to the use condition information on the above 1st included in the auxiliary information set for certification of the restored above 1st, and when it judges that the 2nd above-mentioned processing is continued The above-mentioned data for authentication memorized at the storage step of the above 1st, and the above-mentioned user's proper information memorized at the storage step of the above 2nd, The access rating authentication approach characterized by having the

step which performs predetermined count to the auxiliary information set for certification of the restored above 1st, and generates certification data, and the step which verifies the generated above-mentioned certification data.

[Claim 10] In the auxiliary information generation equipment for certification which generates the auxiliary information for certification that it uses for the access rating authentication equipment which attests the above-mentioned user's access rating by verifying the justification of the certification data generated in order to prove a user's access rating A means to perform predetermined count and to generate the 1st auxiliary information for certification to a user's proper information, the description information on access rating authentication, and the 1st use condition information that described the access condition, A means to encipher the 1st auxiliary information set for certification which consists of auxiliary information for certification on the above 1st, and use condition information on the above 1st, As opposed to the above-mentioned user's proper information, the decode key of the above-mentioned encryption, and the 2nd use condition information that described the access condition Auxiliary information generation equipment for certification characterized by to have a means generate and output the complex auxiliary information for certification from a means performs predetermined count and generate the 2nd auxiliary information for certification, and the 1st auxiliary information set for certification which carried out [above-mentioned] encryption and the auxiliary information set for certification of the above 2nd.

[Claim 11] In the auxiliary information generation method for certification which generates the auxiliary information for certification that it uses for the access rating authentication equipment which attests the above-mentioned user's access rating by verifying the justification of the certification data generated in order to prove a user's access rating The step which performs predetermined count and generates the 1st auxiliary information for certification to a user's proper information, the description information on access rating authentication, and the 1st use condition information that described the access condition, The step which enciphers the 1st auxiliary information set for certification which consists of auxiliary information for certification on the above 1st, and use condition information on the above 1st, The auxiliary information generation method for certification characterized by having the step which performs predetermined count and generates the 2nd auxiliary information for certification to the above-mentioned user's proper information, the decode key of the above-mentioned encryption, and the 2nd use condition information that described the access condition.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the certification data generation equipment which generates especially the above-mentioned certification data about the technique which attests a user's access rating by verifying the justification of the certification data generated in order to prove a user's authority.
[0002]
[Description of the Prior Art] The program execution control technique is known as advanced technology belonging to this invention and an isomerism field. The user who has tried activation of application inspects holding the key for authentication of normal, a program execution control technique embeds the routine for user authentication into ** application program, ** this routine restricts it, when existence of the key for the ** aforementioned authentication is checked, it continues a program, and when other, it is the technique which stops program execution.
[0003] By using such a technique, activation of an application program can be closed to him, if only to the user of the normal which holds an authentication key. It is put in practical use in the software distribution enterprise and this technique is Rainbow as a product. Technologies, SentinelSuperPro (trademark) of an Inc. company, and Aladdin Knowledge Systems There is an HASP (trademark) of a Ltd. company etc.
[0004] With these techniques, a software vendor encloses a user's authentication key with the memory in hardware severely, in order to prevent a duplicate, it is distributed to a user using a postal physical means, and a user equips with and uses this for a proprietary personal computer etc.
[0005] These techniques must perform protection processing of a program based on this authentication key, after a programmer assumes beforehand the authentication key which a user has, when creating an application program. That is, only when the right reply from hardware with a built-in key is predicted at the time of a programming and a right reply is received, a programmer has to create a program so that a program may operate normally.
[0006] The use gestalt of the conventional technique of having such a description becomes the following two kinds fundamentally.
[0007] ** By the 1st approach, prepare a user's authentication key so that it may differ for every user. That is, every one different authentication key for every user is prepared for the user first like authentication **** at authentication **** and the user second.
[0008] ** By the 2nd approach, a programmer prepares an authentication key which is different for every application, respectively. That is, every one authentication key which is different for every application like authentication **** is prepared for the application first at authentication **** and the application second, and each application program is created so that the authentication key of a proper may be identified.
[0009] However, in any [these] case, it has a problem which is described below.
[0010] In the case of the 1st approach, a programmer needs to change the authentication routine in a

program appropriately for every user, and needs to create a program. That is, since authentication keys differ for every user, the authentication routine in a program must be created so that the authentication key of the user proper using this program may be identified, and a programmer needs to create the program from which only the number of use users differs.
[0011] When the target users are a large number, the activity which changes a program an individual exception for every user requires an effort intolerable for a programmer, and becomes what also has a huge list of user authentication keys which must be managed.
[0012] In the case of the 2nd approach, the need of creating a program individually for every user like [in the case of the 1st approach] is lost, but as for a user, only the number of the applications to be used must hold an authentication key conversely.
[0013] As for this constraint, the following problems are caused in a programmer and each user.
[0014] As mentioned above, it is necessary to distribute an authentication key to a user in the condition of having enclosed with hardware severely. Therefore, it cannot but depend for distribution of the hardware which builds an authentication key in that the program itself can be distributed simple through a network, and a contrast target on physical means, such as mail. this limit -- cost, time amount, and the time and effort of packing -- any -- very much -- a programmer -- **** -- it becomes a big burden.
[0015] A programmer has to do the fixed number stock of the different hardware for every application so that he may meet the demand of a user, and he needs the cost of stock control.
[0016] Moreover, a user must be content with the complicatedness that hardware must be exchanged whenever it changes the application to be used.
[0017] Though he wants to use application with a user, it must wait until the hardware with which the authentication key was enclosed arrives, and produces inconvenient [in the point that it cannot use immediately].
[0018] As a technique which solves this problem, these people have proposed the new access rating verification technique (current un-opening [Japanese Patent Application No. No. 062076 / 08 to /,] to the public).
[0019] The description information and user proper information on access rating authentication are made to become independent, and if the protection side and user side also prepares one proper information, he is trying to end by introducing the auxiliary information for certification (access ticket) by the proposal of Japanese Patent Application No. No. 062076 [08 to].
[0020] An access ticket is data calculated based on a specific user's proper information, and the description information on access rating authentication, and is difficult to calculate the description information on access rating authentication for user proper information from an access ticket to not knowing. And the data for right certification are calculated only within the case where the right combination of user proper information and an access ticket, i.e., the combination of the access ticket calculated based on user proper information and this user proper information, is inputted.
[0021] Therefore, access rating of users, such as execution control, can be attested by a user's holding proper information beforehand, and protection persons', such as a programmer's, preparing the description information on access rating authentication independently of the proper information which a user possesses, and creating an access ticket according to a user's proper information and the description information on access rating authentication used for creation of an application program etc., and distributing.
[0022] Using this technique, it protects to an application program, a user is supplied widely, and the service which provides with an access ticket the user who wishes use of an application program can be considered.
[0023] Media, such as an IC card which enclosed different proper information for every user, are passed to the user who wishs, and a programmer distributes to a program using the description information on access rating authentication, protecting, and the ticket issue contractor who received commission in the user who wishes use of a program from the programmer or the programmer offers an access ticket.
[0024] When such service is considered, it becomes a problem how and when it charges. In the case of this example, in case an access ticket is published, the tariff which is equivalent to the price of a

program in exchange for issue of a ticket can be collected.
[0025] By the way, when considering dealing service of the right of use of such a program, the gestalt of the following rights can be considered.
** Purchase (purchase) : how to buy the right of use. Once it purchases, it can use eternally. Then, the tariff is the same in spite of not using.
** Paper youth (pay-per-use) : it is also called the amount accounting of use. It is charged according to the used amount.
** RENTO (rent) : purchase the right of use of a fixed period. If a term passes, it will become impossible to use.
[0026] Although it is easy to realize a purchase when the technique of above-mentioned Japanese Patent Application No. No. 062076 [08 to] is used, it is difficult to realize RENTO.
[0027] Since it is necessary to record the log to the ticket used into a user's IC card in order for a user to submit use hope to a ticket issue contractor every, and ticket issue actuation is frequently needed upwards and to realize an access ticket usable once although a ticket issue contractor can be realized by publishing an access ticket usable once whenever it uses about a paper youth, it is not so realistic.
[0028] To this problem, these people have proposed introducing use control information into the rating authentication technique of an access ticket (current un-opening [Japanese Patent Application No. No. 191756 / 08 to /,] to the public). By the technique of Japanese Patent Application No. No. 191756 [08 to], in case use control information is introduced into Japanese Patent Application No. No. 062076 [08 to] and information is decrypted, this use control information is also used. As an example of use control information, the information on whether the available time the expiration date, the count of usable, and total, the use upper limit amount of money, and the hysteresis of processing are taken etc. is indicated.
[0029] It is possible to realize RENTO, when use control information is the expiration date.
[0030] Moreover, in the case of the information that use control information takes the hysteresis of processing, the function near a paper youth is realizable by the approach of calculating the used count and charging it, by collecting the hysteresis and totaling in a fixed period. If the amount of use per time is furthermore indicated to use control information, it will become possible to realize a flexible paper youth.
[0031] That is, by the technique of Japanese Patent Application No. No. 191756 [08 to], the gestalt purchase, the paper youth, and RENTO of the right mentioned above can all be realized.
[0032] Next, the approach of payment is considered. Following two can be considered as the approach of payment.
[0033] ** How to pay at the time of ticket issue : how to pay, in case a ticket issue contractor publishes an access ticket. A tariff may be recorded by the case where it pays by electronic money, and the issue contractor side, and bank transfer etc. may liquidate.
[0034] ** How to pay by prepaid one : a user purchases prepaid frequency beforehand, holds in the IC card etc., and pull down the frequency which corresponds from prepaid one in the time of purchase, or the case of use.
[0035] If the technique of Japanese Patent Application No. No. 191756 [08 to] is used, the gestalt purchase, the paper youth, and RENTO of the right mentioned above are all realizable by the approach of paying at the time of ** ticket issue.
[0036] On the other hand, by the approach of paying by ** prepaid, a paper youth can be realized easily. every [that is, / given / the prepaid information currently held whenever it attests by indicating the amount of use per time to use control information to / in use control information / frequency] -- what is necessary is just to pull down
[0037] However, it is the approach of paying by ** prepaid, and it is difficult to realize a purchase and RENTO. A purchase carries out accounting by prepaid one only to the first utilization time, and is because processing in which it does not charge is required for the utilization time of the 2nd henceforth.
[0038] About a purchase, indicate the amount of acquisition of the right of use to use control information, and it pulls down from the prepaid information which holds the frame to the first utilization time. The information on the used this access ticket is registered into an IC card. To the utilization time

of the 2nd henceforth Whether the ticket which it is going to use is already registered into the IC card checks, and when registered, it is also possible to realize with constituting so that it may not pull down from prepaid information. However, since it cannot erase during the period, when [very long] using many tickets, this registration information will run short of the storage capacity of an IC card, and is not a not much realistic solution.
[0039] Also in RENTO, the amount of a rental and an expiration date are indicated to use control information, although it is possible, similarly realizing by taking the same approach as a purchase will run short of the storage capacity of an IC card, and it is not a not much realistic solution.
[0040]
[Problem(s) to be Solved by the Invention] This invention is made in view of the above troubles, and it makes it a technical problem to make it possible to realize a purchase and RENTO also in the approach of paying by prepaid one, without covering an excessive load over a certification data generation equipment (IC card) side.
[0041]
[Means for Solving the Problem] A data input means for authentication to input the data for authentication into the certification data generation equipment which is generated in order to attest a user's access rating, and generates the certification data which have justification verified in order to solve an above-mentioned technical problem according to this invention, A user proper information storage means to memorize a user's proper information, and a user's proper information, The auxiliary information for certification which performed and generated predetermined count to the description information on access rating authentication, and the use condition information which described the access condition, An auxiliary information set storage means for certification to memorize the auxiliary information set for certification containing a group with use condition information, The auxiliary information set for certification corresponding to the inputted data for authentication is taken out from the above-mentioned auxiliary information set storage means for certification. The above-mentioned picking when it is judged as continuation in a use conditional-judgment means to judge whether subsequent processings are continued, and the above-mentioned use conditional-judgment means, according to the use condition information on the taken-out auxiliary information set for certification The above-mentioned picking The taken-out auxiliary information set for certification, and the data for authentication inputted from the above-mentioned data input means for authentication, Perform predetermined count to the above-mentioned user's proper information memorized by the above-mentioned user proper information storage means, and a certification data generation output means to generate and output certification data is established. From the above-mentioned data input means for authentication, the auxiliary information set for encryption certification which enciphered the 1st auxiliary information set for certification with the encryption key in a code function is inputted. The above-mentioned use conditional-judgment means The 2nd auxiliary information set for certification corresponding to the inputted auxiliary information set for encryption certification is taken out from the above-mentioned auxiliary information set storage means for certification. After performing predetermined processing according to the use condition information on the 2nd auxiliary information set for certification taken [above-mentioned] out picking, it judges whether subsequent processings are continued. The above-mentioned certification data generation output means He is trying to output the 1st auxiliary information set for certification which is the result of decrypting the above-mentioned auxiliary information set for encryption certification by performing the above-mentioned processing.
[0042] That is, the 1st auxiliary information set for certification is decrypted from the auxiliary information set for encryption certification by enciphering the 1st auxiliary information set for certification which is the usual auxiliary information set for certification (access ticket), creating the auxiliary information set for encryption certification, and carrying out the completely same processing as the usual authentication processing using the 2nd auxiliary information set for certification for accessing to this auxiliary information set for encryption certification.
[0043] Thus, by constituting, a use tariff creates a free ticket (1st auxiliary information set for certification), it enciphers, and implementation of the purchase function in prepaid one is made possible

as a whole by constituting so that the ticket (2nd auxiliary information set for certification) for decrypting the enciphered ticket may be published, the use tariff of this ticket (2nd auxiliary information set for certification) may be made into the charge and it may pay by prepaid one.
[0044] A RENTO function is realizable by indicating expiration date information to the use condition information on the 2nd auxiliary information set for certification in addition to this.
[0045] In addition, realizing efficiently is possible, without putting in an excessive program and data in an IC card with comparatively little capacity, since it constituted so that the same processing as authentication processing of the usual ticket might be performed in order to have decrypted the enciphered ticket.
[0046]
[Embodiment of the Invention] Hereafter, the example of this invention is explained.
[0047] Drawing 1 shows the block diagram of this example. In this example, prepaid information is held in certification data generation equipment, and the example (purchase) which purchases the access privilege of an application program is explained using that prepaid information.
[0048] Drawing 1 shows including the certification data verification equipment which verifies the certification data generated and outputted with certification data generation equipment.
[0049] First, after explaining the configuration of this example based on drawing 1 , while a flow chart shows the flow of processing of certification data verification equipment and certification data generation equipment, it explains. It explains to an example by carrying out authentication processing usual to explanation of the flow of processing, and the example pulled down from prepaid one for whenever [of one use to the use condition information L / every] is explained. And the example (purchase) which purchases the access privilege of an application program after explanation of the usual authentication processing is explained.
[0050] It is equipment of the pocket mold which [configuration of example] drawing 1 shows the configuration of an example as a whole, and a user holds certification data generation equipment 10 in this drawing, and had a count function in the interior like an IC card. The PC card which had a count function besides the IC card, a pocket mold information tool or a subnote PC, etc. may be used. It is desirable to be defended so that information on internal may not be simply altered from the outside.
[0051] A user is the personal computer which uses an application program, and certification data verification equipment 20 equips with and uses the IC card which is certification data generation equipment 10 for the slot of a personal computer.
[0052] Certification data verification equipment 20 consists of the data generation section 21 for authentication, and the certification data verification section 22 greatly. When needing to be attested, the data generation section 21 for authentication generates the data for authentication, and sends them to certification data generation equipment 10. The certification data with which the certification data verification section 22 was returned from certification data generation equipment 10 verify whether it is the right.
[0053] If it is protected by encryption etc. and a user is going to use an application program, an application program will restrict certification data-verification equipment 20, when the data for authentication corresponding to the application program are created, the certification data returned to certification data generation equipment 10 from delivery and certification data generation equipment 10 are verified and it is verified with the right, and will make it possible to remove and use protection of an application program.
[0054] On the other hand, certification data generation equipment 10 is constituted including the user proper information storage section 11, the frequency information attaching part 12, the access ticket storage section 13, the data input section 14 for authentication, the use conditional-judgment section 15, and the certification data generation output section 16.
[0055] The user proper information storage section 11 is a part holding a user's confidential information, and is different information for every user. As for user proper information, it is desirable to be constituted so that it may be enclosed when certification data generation equipment 10 is created, and it cannot take out to a user, either.

[0056] The frequency information attaching part 12 is a part holding prepaid information, and the required frame is reduced according to use, purchase, etc. of an application program. Increasing is also possible when a frame decreases. The technique proposed by Japanese Patent Application No. No. 21373 [nine to] can be used for the approach of increase. By this technique, frequency information is increased using frequency information and the frequency information which signed. It is required to carry out the change in the frame in the frequency information attaching part 12 to insurance, and it is desirable to constitute so that access of those other than the defined approach cannot be performed.
[0057] The access ticket storage section 13 has memorized two or more access tickets. An access ticket gives a user access rating and is created by the ticket issue contractor who received commission from the application program implementer or the application program implementer. In this example, an access ticket is the group of the auxiliary information for certification and use condition information which were calculated by performing predetermined count to a user's proper information, the description information on access rating authentication, and the use condition information that described the access condition of access rating authentication. Although the access ticket storage section is constituted in the IC card, since only he who was published can use an access ticket, the copy is free and may consist of this examples in the IC card exterior.
[0058] The data input section 14 for authentication is a part which inputs the data for authentication sent from certification data verification equipment 20.
[0059] The use conditional-judgment section 15 takes out the access ticket corresponding to the inputted data for authentication from the access ticket storage section 13, and judges use conditions based on the use condition information in an access ticket. For example, it judges [whether the expiration date of an access ticket has run out or it is sufficient for paying a use tariff by prepaid one which it holds and] whether use conditions are judged and subsequent processings are continued.
[0060] The certification data generation output section 16 generates and outputs certification data, only when judged as continuation in the use conditional-judgment section 15. Certification data perform and create predetermined count to the auxiliary information for certification in the access ticket taken out in the use conditional-judgment section 15, the data for authentication, and a user's proper information.
[0061] Next, an example is given and it explains to a detail further. Explanation here makes the usual authentication processing an example, explains, and explains to the use condition information L the example pulled down from prepaid one for whenever [of one use / every].
[0062] Drawing 2 attaches a notation to the block diagram of drawing 1 . The notation corresponds with the following explanation.
[0063] below the [usual authentication processing] -- law -- the example using the RSA (Rivest-Shamir-Adelman) code in n is explained to a detail. First, the usual authentication processing is explained. In the following examples, the software vendor which is the implementer of an application program explains the example which performs all from issue of an IC card to issue of a ticket. In this example, the software vendor knows all users' confidential information du. The configuration whose ticket issue contractor performs issue of an IC card and a ticket besides this is also possible.
[0064] A software vendor creates the cryptographic key to an application program to protect. since RSA cryptograph is used here -- the big prime factors p and q -- secret -- creating -- law -- a number n is created as n=p-q. next, law -- the origin of a number n -- a cryptographic key E and the decode key D -- [0065]
[Equation 1] ED**1 mod phi (n)
******** -- it generates like. phi (n) is the Euler number and is phi(n) = (p-1) (q-1) here.
[0066] Next, a software vendor enciphers a part or all of an application program that wants to make and protect the common cryptographic key K by K, and is [0067].
[Equation 2] K'=KE mod n is calculated, and it embeds and distributes to the application program which enciphered K' so that the 3rd person cannot take out.
[0068] The user who wants to use this application program will receive the access ticket corresponding to this beforehand.
[0069] A software vendor publishes an access ticket in response to the access ticket issue demand from a

user. A software vendor picks out the confidential information du of the user who required, and the decode key (D, n) corresponding to the cryptographic key (E, n) used on the occasion of encryption of an application program from a database. Next, the use condition information L given to an access ticket is created. Here, since it pulls down from prepaid one and charges, the amount of use pulled down about one use is set to L. And such information is used and it is [0070].
[Equation 3] t=D-F(n,L,du)
It carries out and the auxiliary information t for certification is created. On the other hand, function F() is the function of tropism, and, on the other hand, can use tropism Hash Function MD5, SHA, etc. a common key encryptosystem DES (DataEncryption Standard), etc. here.
[0071] A software vendor is published to a user by using the group of (t, L, n) as an access ticket.
[0072] If a user is going to use an application program, certification data verification equipment will create the data for authentication corresponding to the application program (C, n), and will send them to certification data generation equipment.
[0073] The flow of this processing is shown in the flow chart of drawing 3 , and it explains based on this.
: (Step S11) The certification data generation section 21 takes out K' and n from the protected application program.
: (Step S12) The certification data generation section generates a random number r, and stores it in a random-number attaching part.
(Step S13) :C=rEK' mod n is calculated.
(Step S14) It sends to certification data generation equipment 10 by using the group of : (C, n) as the data for authentication.
[0074] Next, the flow of certification data generation equipment 10 is shown in drawing 4 , and processing of certification data generation equipment 10 is explained based on this.
: (Step S21) The data for authentication (C, n) are inputted from the data input section 14 for authentication.
: (Step S22) The use conditional-judgment section 15 uses n as a key, searches the access ticket storage section, and takes out an access ticket (t, L, n).
: (Step S23) The use conditional-judgment section 15 compares the frequency information V on the use conditions L in the taken-out access ticket (amount of use), and a frequency information attaching part.
: (Steps S24-S25) At the time of V>=L, the certification data generation output section 16 progresses to (step S26). When that is not right, the certification data generation output section outputs an error, and is completed.
: (Step S26) Only the part of the use conditions (amount of use) L reduces the frequency information V for which the use conditional-judgment section 15 is held at the frequency information attaching part 12.

: (Steps S26-S29) The certification data generation output section 16 calculates and outputs the certification data R using the auxiliary information t for certification which the use conditional-judgment section 15 took out, the use conditions L (amount of use), and du read from the user proper information storage section 11.
[0075]
[Equation 4] R'=CF (n, L, du) mod nR=CtR' mod In n drawing 4 , although the certification data R are calculated, count of R' is once divided. In order for this to use a user's confidential information for count of R', it is necessary to calculate but so that the processing may not leak outside, and once count of R' finishes, it will be for performing count of R externally. Thus, you may calculate by dividing into R' and R, and it does not matter even if it calculates at once.
[0076] Next, processing of the certification data verification section of certification data verification equipment 20 is explained. The certification data R outputted from certification data generation equipment 10 are [the right user proper information du and] [0077] when calculated using a right access ticket (the auxiliary information t for right certification, the right use conditions L).
[Equation 5]

R=CtR' mod n=CD-F(n, L, du) CF(n, L, du) mod n=CD mod n=(rE K') D mod n=(rEKE) D mod n=(rK) ED mod It becomes n=rK.
[0078] Then, in the certification data verification section 22, a random number r is taken out from the random-number attaching part 23, and it is [0079].
[Equation 6] r-1R mod By calculating n, the common cryptographic key K which had enciphered application can come to hand. Certification data verification equipment can decode the part as which application was enciphered by this common cryptographic key K, and can perform application.
[0080] In this example, certification data verification equipment has that application has performed correctly, and it is judged that verification was completed correctly.
[0081] Explanation of the usual authentication processing is ended above.
[0082] The example (purchase) which purchases the access privilege of an application program is explained using a [purchase], next prepaid information.
[0083] In order to realize this function, the 1st access ticket is decrypted from an encryption access ticket by enciphering the 1st access ticket which is the usual access ticket, creating the encryption access ticket, and performing the completely same processing as the usual authentication processing using the 2nd access ticket for accessing to this encryption access ticket.
[0084] And at this time, a use tariff creates the 1st access ticket as a free ticket, and the 2nd access ticket is constituting so that a use tariff's may be made into the charge and it may pay by prepaid one, and enables implementation of the purchase function in prepaid one as a whole.
[0085] First, the application program which wants to realize the function of a purchase is set to AP1. AP1 is protected like above-mentioned explanation.
[0086] A <explanation of protection of application program AP 1> software vendor creates the cryptographic key to an application program to protect. since RSA cryptograph is used here -- the big prime factors p1 and q1 -- secret -- creating -- law -- an n1 number is created as n1=p1 and q1. next, law -- the origin of an n1 number -- a cryptographic key E1 and the decode key D1 -- [0087]
[Equation 7] E1 and D 1**1 mod phi (n1)
******** -- it generates like. phi (n1) is the Euler number and is phi(n1) = (p1-1) (q1-1) here.
[0088] Next, a software vendor enciphers a part or all of an application program that wants to make and protect the common cryptographic key K1 by K1, enciphers the common cryptographic key K1 by the cryptographic key E1 according to the following formulas further, and generates K1'.
[0089]
[Equation 8] It embeds and distributes to the application program which enciphered K1'=K1E1 mod n1 and K1' so that the 3rd person cannot take out easily. Moreover, n1 is embedded at the enciphered application program.
[0090] A software vendor memorizes the group created (n1, D1, phi (n1)) in an access ticket information database.
[0091] Next, creation of a prepaid payment purchase ticket is explained. Drawing 5 shows the example of a configuration of the auxiliary information generation equipment 30 for certification. In this example, a prepaid payment purchase ticket is outputted by considering the 1st use condition information, the 1st decode key, user proper information, and 2nd use condition information as an input. In drawing 5 , the input section 31 is a part which inputs the 1st use condition information, the 1st decode key, user proper information, and the 2nd use condition information. The 1st decode key storage section 33 is a part which memorizes the 1st decode key inputted from the input section 31. The 1st decode key is a decode key (D1, n1) corresponding to the cryptographic key (E1, n1) which enciphered the common cryptographic key K1 used for encryption of an application program AP 1.
[0092] The user proper information storage section 34 is a part which memorizes the user proper information that it was inputted from the input section 31. This is the same as that of what is stored in a user's certification data generation equipment 10.
[0093] When a user requests issue of a ticket, a user's identification information U and a user send n1 taken out from the application program AP 1 which wishes to use to a software vendor. A software vendor from the User Information database which matches and holds a user's identification information

U and user proper information du User proper information is acquired by retrieving the user proper information du corresponding to a user's identification information U. From the access ticket information database holding a group, the decode key (D1, n1) corresponding to n1 is obtained, and moreover (n, D, phi (n)) inputs into the auxiliary information generation equipment 30 for certification.
[0094] The 1st use condition information storage section 32 and the 2nd use condition information storage section 35 are parts which memorize the 1st use condition information and the 2nd use condition information, respectively. The 1st use condition information describes the use conditions of an application program AP 1, and the 2nd use condition information describes the use conditions of a prepaid payment purchase ticket. In the case of the prepaid payment purchase ticket, since it is charged at the 1st utilization time and has the property of not being charged in the utilization time of the 2nd henceforth, the information meaning being no charge at least is included in the 1st use condition information, and the information meaning being a charge at least is included at the 2nd use condition information.
[0095] The 1st ticket generation section 36 is a part which performs predetermined count to the 1st use condition information and the 1st decode key which were inputted, and user proper information, and generates an access ticket.
[0096] The component 41 which consists of the 1st use condition information storage section 32, the 1st decode key storage section 33, the user proper information storage section 34, and the 1st ticket generation section 36 is making the configuration same with generating the usual access ticket.
[0097] The 2nd key generation section 37 is a part which generates the key for enciphering the 1st access ticket generated in the 1st ticket generation section 36.
[0098] The encryption section 38 is a part which enciphers the 1st access ticket generated in the 1st ticket generation section 36 using the encryption key generated in the 2nd key generation section 37.
[0099] The 2nd ticket generation section 39 is a part which generates the 2nd access ticket which is needed in order to decrypt the encryption access ticket enciphered in the encryption section 38.
[0100] The ticket output section 40 is outputted as a prepaid payment purchase ticket combining the encryption access ticket enciphered in the encryption section 38, and the 2nd access ticket generated in the 2nd ticket generation section 39.
[0101] The approach of creation of a prepaid payment purchase ticket is explained below to <creation of a prepaid payment purchase ticket> using the flow chart of drawing 6 .
[0102] A software vendor publishes a prepaid payment purchase ticket in response to the prepaid payment purchase ticket issue demand from a user. The user who requests issue of a ticket sends n1 taken out from the application program AP 1 with which a user's identification information U and a user wish to use to a software vendor.
[0103] : (Step S31) A software vendor inputs the group (U, n1) of n1 taken out from identification information U and application program AP 1 of the user who is the prepaid payment purchase ticket issue demand from a user. Moreover, the 1st use condition information L1 which described the use conditions of an application program AP 1, and the 2nd use condition information L2 which described the use conditions of a prepaid payment purchase ticket are also inputted. Here, it is [0104] as which the 1st use condition information L1 means that a use tariff is no charge since it aims at generation of a prepaid payment purchase ticket.
[Equation 9] It is [0105] as which it is L1=0 and the 2nd use condition information L2 means that the tariff of a purchase is a charge.
[Equation 10] It is referred to as L2=A. However, A is figures other than zero, for example, is 100.
[0106] : (Step S32) The user proper information du corresponding to a user's identification information U is retrieved from the User Information database which matches and holds a user's identification information U and user proper information du.
(Step S33) From the access ticket information database holding the group of : (n, D, phi (n)), the 1st decode key (D1, n1) corresponding to n1 is searched.
: (Step S34) The 1st access ticket T1 for a user to access AP1 is created.
[0107]

[Equation 11] T1=(t1,L1,n1)
t1=D1-F(n1,L1,du)
(Step S35) : -- in order to encipher the 1st access ticket T1 -- the 2nd law -- an n2 number, the 2nd cryptographic key E2, and the 2nd decode key D2 are generated. the big prime factors p2 and q2 are generated, and the following formulas are realized -- as -- law -- an n2 number, a cryptographic key E2, and the decode key D2 are generated.
[0108]
[Equation 12] n2=p2, q2E2, and D 2**1 mod phi (n2)
phi(n2) = (p2-1) (q2-1)
: (Step S36) The 1st access ticket T1 is enciphered by the 2nd generated cryptographic key E2. What enciphered T1 is made into T1'.
[0109]
[Equation 13] T1'=T1E2 mod n2 (step S37): Create the 2nd access ticket T2 for a user to decode enciphered access ticket T1'.
[0110]
[Equation 14] T2=(t2,L2,n2)
t2=D2-F(n2,L2,du)
(Step S38) : (T1', n2) (T2) is made into a group, and it outputs as a prepaid payment purchase ticket.
[0111] A software vendor sends the outputted prepaid payment purchase ticket (T1', n2) (T2) to a user.
[0112] Next, the example of use of a prepaid payment purchase ticket is explained.
[0113] The user who received the (example a) prepaid payment purchase ticket (T1', n2) (T2) stores T2 in the access ticket storage section 13 first. [<example of use of prepaid payment purchase ticket>]
(b) Next, input from the data input section 14 for authentication of the certification data generation equipment 10 with which he holds (T1', n2).
[0114] Hereafter, processing in certification data generation equipment 10 is performed according to drawing 4 . Now, suppose at the frequency information attaching part 12 of certification data generation equipment 14 that the prepaid information V on 800 frequencies is held. (V=800)
: (Step S21) From the data input section 14 for authentication, the data for authentication (T1', n2) are inputted.
: (Step S22) The use conditional-judgment section 15 uses n2 as a key, searches the access ticket storage section 13, and takes out access ticket T2= (t2, L2, n2).
: (Step S23) The use conditional-judgment section 15 compares the frequency information V on the frequency information attaching part 12 with the use conditions L2 in the taken-out access ticket.
: (Step S24) Since it is now, L2=100, and V= 800, it is [0115].
[Equation 15] V>=L2 is realized and it progresses to (step S26).
: (Step S26) Only the part of the use conditions L2 reduces the frequency information V for which the use conditional-judgment section 15 is held at the frequency information attaching part 12.
[0116]
[Equation 16] As an acquisition tariff of a prepaid payment purchase ticket, V=800-100=700 [V], i.e., frequency information, are pulled down the number of 100 degrees, and it serves as remainder 700 frequency.
: (Steps S27-S29) The certification data generation output section 16 calculates and outputs the certification data R using the auxiliary information t2 for certification and the use conditions L2 which the use conditional-judgment section 15 took out, and du read from the user proper information storage section 11.
[0117]
[Equation 17] R'=T1'F (n2, L2, du) mod n2R=T1't2R' mod It is [0118] when n2R is calculated.
[Equation 18]
R=T1't2R' mod n2=T1'D2-F(n2, L2, du) CF(n2, L2, du) mod n2=T1' D2 mod n2=(T1 E2) D2 mod Count called n2=T1 is realized and it is [0119] as certification data R from the certification data generation output section 16.

[Equation 19] R=T1 is outputted.
[0120] That is, if it inputs from the data input section 14 for authentication of the certification data generation equipment 10 with which he holds (T1', n2), L2 will be pulled down from the frequency information V, and T1 by which T1' was decoded as a result will be outputted.
[0121] (c) A user stores T1 which came to hand in the access ticket storage section 13.
[0122] (d) Since the user obtained the access ticket T1 for using an application program AP 1, he uses an application program AP 1.
[0123] Hereafter, data generation processing for authentication in certification data verification equipment 10 is performed according to drawing 3 .
: (Step S11) The data generation section 21 for authentication takes out K1' and n1 from the protected application program.
: (Step S12) The data generation section 21 for authentication generates a random number r, and stores it in the random-number attaching part 23.
(Step S13) :C=rEK1' mod n1 is calculated.
(Step S14) It sends to certification data generation equipment 10 by using the group of : (C, n1) as the data for authentication.
(e) Processing in certification data generation equipment 10 is again performed according to drawing 4 .
: (Step S21) From the data input section 14 for authentication, the data for authentication (C, n1) are inputted.
: (Step S22) The use conditional-judgment section 15 uses n1 as a key, searches the access ticket storage section 13, and takes out access ticket T1= (t1, L1, n1).
: (Step S23) The use conditional-judgment section 15 compares the frequency information V on the frequency information attaching part 12 with the use conditions L1 in the taken-out access ticket.
: (Step S24) Since it is now, L1=0, and V= 700, it is [0124].
[Equation 20] V>=L1 is realized and it progresses to (step S26).
: (Step S26) Only the part of the use conditions L1 reduces the frequency information V for which the use conditional-judgment section 15 is held at the frequency information attaching part 12.
[0125]
[Equation 21] First, as an acquisition tariff of a prepaid payment purchase ticket, since V=700-0=700 [V], i.e., frequency information, are pulled down the number of 100 degrees, by use of the 2nd henceforth, it is not pulled down but serves as as [remainder 700 frequency].
: (Steps S27-S29) The certification data generation output section 16 calculates and outputs the certification data R using the auxiliary information t1 for certification and the use conditions L1 which the use conditional-judgment section 15 took out, and du read from the user proper information storage section 11.
[0126]
[Equation 22] R'=CF(n1, L1, du) mod n1R=Ct1R' mod n1, i.e., [0127]
[Equation 23]
R=Ct1R' mod The certification data verification section 22 of n1=rK(f) certification data verification equipment 20 processes like the usual authentication, takes out a random number r from the random-number attaching part 23, and is [0128].
[Equation 24] r-1R mod By calculating n1, the common cryptographic key K which had enciphered application can come to hand. Certification data verification equipment can decode the part as which application was enciphered by this common cryptographic key K, and can perform application.
[0129] After this, even if it performs an application program AP 1 what times, same processing is performed and it can use for free.
[0130] As explained above, what (purchase) the access privilege of an application program is purchased for with constituting as mentioned above using prepaid information becomes possible.
[0131] In the above, implementation of the purchase function in prepaid one was explained.
[0132] When certification data generation equipment is equipped with a clock, and in addition to the information of no charge the amount of use indicates expiration date information and compares with

time of day in the use condition information L on the 1st access ticket at every use of the 1st access ticket besides this, it is also possible to realize the RENTO function in prepaid one.
[0133] Furthermore, it is possible to limit the term which distributes the 1st access ticket (defrosting) etc. by equipping certification data generation equipment with a clock, and comparing with time of day as another example, in the case of decode of the 1st access ticket which indicated expiration date information in the use condition information L on the 2nd access ticket, and was enciphered.
[0134] Moreover, although this example explained by carrying out based on RSA cryptograph, not only this but other cipher systems may be used. Moreover, the implementation type of an access ticket is not restricted to this, either.
[0135]
[Effect of the Invention] Face attesting access rating of users, such as execution control, and a user holds proper information beforehand. Protection persons, such as a programmer, prepare the description information on access rating authentication independently of the proper information which a user possesses. By creating and distributing an access ticket according to a user's proper information and the description information on the access rating authentication used for creation of an application program etc. It made it possible to realize the purchase function and RENTO function in difficult prepaid one conventionally, with the description of making the both sides of a user and a protection person open wide from the troublesomeness of access privilege information management left.
[0136] Realizing efficiently is possible, without putting in an excessive program and data in an IC card with comparatively little capacity, since it constituted so that it might set to realize these functions furthermore and the same processing as authentication processing of the usual ticket might be performed.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL FIELD

[Field of the Invention] This invention relates to the certification data generation equipment which generates especially the above-mentioned certification data about the technique which attests a user's access rating by verifying the justification of the certification data generated in order to prove a user's authority.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

PRIOR ART

[Description of the Prior Art] The program execution control technique is known as advanced technology belonging to this invention and an isomerism field. The user who has tried activation of application inspects holding the key for authentication of normal, a program execution control technique embeds the routine for user authentication into ** application program, ** this routine restricts it, when existence of the key for the ** aforementioned authentication is checked, it continues a program, and when other, it is the technique which stops program execution.
[0003] By using such a technique, activation of an application program can be closed to him, if only to the user of the normal which holds an authentication key. It is put in practical use in the software distribution enterprise and this technique is Rainbow as a product. Technologies, SentinelSuperPro (trademark) of an Inc. company, and Aladdin Knowledge Systems There is an HASP (trademark) of a Ltd. company etc.
[0004] With these techniques, a software vendor encloses a user's authentication key with the memory in hardware severely, in order to prevent a duplicate, it is distributed to a user using a postal physical means, and a user equips with and uses this for a proprietary personal computer etc.
[0005] These techniques must perform protection processing of a program based on this authentication key, after a programmer assumes beforehand the authentication key which a user has, when creating an application program. That is, only when the right reply from hardware with a built-in key is predicted at the time of a programming and a right reply is received, a programmer has to create a program so that a program may operate normally.
[0006] The use gestalt of the conventional technique of having such a description becomes the following two kinds fundamentally.
[0007] ** By the 1st approach, prepare a user's authentication key so that it may differ for every user. That is, every one different authentication key for every user is prepared for the user first like authentication **** at authentication **** and the user second.
[0008] ** By the 2nd approach, a programmer prepares an authentication key which is different for every application, respectively. That is, every one authentication key which is different for every application like authentication **** is prepared for the application first at authentication **** and the application second, and each application program is created so that the authentication key of a proper may be identified.
[0009] However, in any [these] case, it has a problem which is described below.
[0010] In the case of the 1st approach, a programmer needs to change the authentication routine in a program appropriately for every user, and needs to create a program. That is, since authentication keys differ for every user, the authentication routine in a program must be created so that the authentication key of the user proper using this program may be identified, and a programmer needs to create the program from which only the number of use users differs.
[0011] When the target users are a large number, the activity which changes a program an individual exception for every user requires an effort intolerable for a programmer, and becomes what also has a huge list of user authentication keys which must be managed.

[0012] In the case of the 2nd approach, the need of creating a program individually for every user like [in the case of the 1st approach] is lost, but as for a user, only the number of the applications to be used must hold an authentication key conversely.
[0013] As for this constraint, the following problems are caused in a programmer and each user.
[0014] As mentioned above, it is necessary to distribute an authentication key to a user in the condition of having enclosed with hardware severely. Therefore, it cannot but depend for distribution of the hardware which builds an authentication key in that the program itself can be distributed simple through a network, and a contrast target on physical means, such as mail. this limit -- cost, time amount, and the time and effort of packing -- any -- very much -- a programmer -- **** -- it becomes a big burden.
[0015] A programmer has to do the fixed number stock of the different hardware for every application so that he may meet the demand of a user, and he needs the cost of stock control.
[0016] Moreover, a user must be content with the complicatedness that hardware must be exchanged whenever it changes the application to be used.
[0017] Though he wants to use application with a user, it must wait until the hardware with which the authentication key was enclosed arrives, and produces inconvenient [in the point that it cannot use immediately].
[0018] As a technique which solves this problem, these people have proposed the new access rating verification technique (current un-opening [Japanese Patent Application No. No. 062076 / 08 to /,] to the public).
[0019] The description information and user proper information on access rating authentication are made to become independent, and if the protection side and user side also prepares one proper information, he is trying to end by introducing the auxiliary information for certification (access ticket) by the proposal of Japanese Patent Application No. No. 062076 [08 to].
[0020] An access ticket is data calculated based on a specific user's proper information, and the description information on access rating authentication, and is difficult to calculate the description information on access rating authentication for user proper information from an access ticket to not knowing. And the data for right certification are calculated only within the case where the right combination of user proper information and an access ticket, i.e., the combination of the access ticket calculated based on user proper information and this user proper information, is inputted.
[0021] Therefore, access rating of users, such as execution control, can be attested by a user's holding proper information beforehand, and protection persons', such as a programmer's, preparing the description information on access rating authentication independently of the proper information which a user possesses, and creating an access ticket according to a user's proper information and the description information on access rating authentication used for creation of an application program etc., and distributing.
[0022] Using this technique, it protects to an application program, a user is supplied widely, and the service which provides with an access ticket the user who wishes use of an application program can be considered.
[0023] Media, such as an IC card which enclosed different proper information for every user, are passed to the user who wishs, and a programmer distributes to a program using the description information on access rating authentication, protecting, and the ticket issue contractor who received commission in the user who wishes use of a program from the programmer or the programmer offers an access ticket.
[0024] When such service is considered, it becomes a problem how and when it charges. In the case of this example, in case an access ticket is published, the tariff which is equivalent to the price of a program in exchange for issue of a ticket can be collected.
[0025] By the way, when considering dealing service of the right of use of such a program, the gestalt of the following rights can be considered.
** Purchase (purchase) : how to buy the right of use. Once it purchases, it can use eternally. Then, the tariff is the same in spite of not using.
** Paper youth (pay-per-use) : it is also called the amount accounting of use. It is charged according to the used amount.

** RENTO (rent) : purchase the right of use of a fixed period. If a term passes, it will become impossible to use.
[0026] Although it is easy to realize a purchase when the technique of above-mentioned Japanese Patent Application No. No. 062076 [08 to] is used, it is difficult to realize RENTO.
[0027] Since it is necessary to record the log to the ticket used into a user's IC card in order for a user to submit use hope to a ticket issue contractor every, and ticket issue actuation is frequently needed upwards and to realize an access ticket usable once although a ticket issue contractor can be realized by publishing an access ticket usable once whenever it uses about a paper youth, it is not so realistic.
[0028] To this problem, these people have proposed introducing use control information into the rating authentication technique of an access ticket (current un-opening [Japanese Patent Application No. No. 191756 / 08 to /,] to the public). By the technique of Japanese Patent Application No. No. 191756 [08 to], in case use control information is introduced into Japanese Patent Application No. No. 062076 [08 to] and information is decrypted, this use control information is also used. As an example of use control information, the information on whether the available time the expiration date, the count of usable, and total, the use upper limit amount of money, and the hysteresis of processing are taken etc. is indicated.
[0029] It is possible to realize RENTO, when use control information is the expiration date.
[0030] Moreover, in the case of the information that use control information takes the hysteresis of processing, the function near a paper youth is realizable by the approach of calculating the used count and charging it, by collecting the hysteresis and totaling in a fixed period. If the amount of use per time is furthermore indicated to use control information, it will become possible to realize a flexible paper youth.
[0031] That is, by the technique of Japanese Patent Application No. No. 191756 [08 to], the gestalt purchase, the paper youth, and RENTO of the right mentioned above can all be realized.
[0032] Next, the approach of payment is considered. Following two can be considered as the approach of payment.
[0033] ** How to pay at the time of ticket issue : how to pay, in case a ticket issue contractor publishes an access ticket. A tariff may be recorded by the case where it pays by electronic money, and the issue contractor side, and bank transfer etc. may liquidate.
[0034] ** How to pay by prepaid one : a user purchases prepaid frequency beforehand, holds in the IC card etc., and pull down the frequency which corresponds from prepaid one in the time of purchase, or the case of use.
[0035] If the technique of Japanese Patent Application No. No. 191756 [08 to] is used, the gestalt purchase, the paper youth, and RENTO of the right mentioned above are all realizable by the approach of paying at the time of ** ticket issue.
[0036] On the other hand, by the approach of paying by ** prepaid, a paper youth can be realized easily. every [that is, / given / the prepaid information currently held whenever it attests by indicating the amount of use per time to use control information to / in use control information / frequency] -- what is necessary is just to pull down
[0037] However, it is the approach of paying by ** prepaid, and it is difficult to realize a purchase and RENTO. A purchase carries out accounting by prepaid one only to the first utilization time, and is because processing in which it does not charge is required for the utilization time of the 2nd henceforth.
[0038] About a purchase, indicate the amount of acquisition of the right of use to use control information, and it pulls down from the prepaid information which holds the frame to the first utilization time. The information on the used this access ticket is registered into an IC card. To the utilization time of the 2nd henceforth Whether the ticket which it is going to use is already registered into the IC card checks, and when registered, it is also possible to realize with constituting so that it may not pull down from prepaid information. However, since it cannot erase during the period, when [very long] using many tickets, this registration information will run short of the storage capacity of an IC card, and is not a not much realistic solution.
[0039] Also in RENTO, the amount of a rental and an expiration date are indicated to use control information, although it is possible, similarly realizing by taking the same approach as a purchase will

run short of the storage capacity of an IC card, and it is not a not much realistic solution.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

EFFECT OF THE INVENTION

[Effect of the Invention] Face attesting access rating of users, such as execution control, and a user holds proper information beforehand. Protection persons, such as a programmer, prepare the description information on access rating authentication independently of the proper information which a user possesses. By creating and distributing an access ticket according to a user's proper information and the description information on the access rating authentication used for creation of an application program etc. It made it possible to realize the purchase function and RENTO function in difficult prepaid one conventionally, with the description of making the both sides of a user and a protection person open wide from the troublesomeness of access privilege information management left.
[0136] Realizing efficiently is possible, without putting in an excessive program and data in an IC card with comparatively little capacity, since it constituted so that it might set to realize these functions furthermore and the same processing as authentication processing of the usual ticket might be performed.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention] This invention is made in view of the above troubles, and it makes it a technical problem to make it possible to realize a purchase and RENTO also in the approach of paying by prepaid one, without covering an excessive load over a certification data generation equipment (IC card) side.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

MEANS

[Means for Solving the Problem] A data input means for authentication to input the data for authentication into the certification data generation equipment which is generated in order to attest a user's access rating, and generates the certification data which have justification verified in order to solve an above-mentioned technical problem according to this invention, A user proper information storage means to memorize a user's proper information, and a user's proper information, The auxiliary information for certification which performed and generated predetermined count to the description information on access rating authentication, and the use condition information which described the access condition, An auxiliary information set storage means for certification to memorize the auxiliary information set for certification containing a group with use condition information, The auxiliary information set for certification corresponding to the inputted data for authentication is taken out from the above-mentioned auxiliary information set storage means for certification. The above-mentioned picking when it is judged as continuation in a use conditional-judgment means to judge whether subsequent processings are continued, and the above-mentioned use conditional-judgment means, according to the use condition information on the taken-out auxiliary information set for certification The above-mentioned picking The taken-out auxiliary information set for certification, and the data for authentication inputted from the above-mentioned data input means for authentication, Perform predetermined count to the above-mentioned user's proper information memorized by the above-mentioned user proper information storage means, and a certification data generation output means to generate and output certification data is established. From the above-mentioned data input means for authentication, the auxiliary information set for encryption certification which enciphered the 1st auxiliary information set for certification with the encryption key in a code function is inputted. The above-mentioned use conditional-judgment means The 2nd auxiliary information set for certification corresponding to the inputted auxiliary information set for encryption certification is taken out from the above-mentioned auxiliary information set storage means for certification. After performing predetermined processing according to the use condition information on the 2nd auxiliary information set for certification taken [above-mentioned] out picking, it judges whether subsequent processings are continued. The above-mentioned certification data generation output means He is trying to output the 1st auxiliary information set for certification which is the result of decrypting the above-mentioned auxiliary information set for encryption certification by performing the above-mentioned processing.
[0042] That is, the 1st auxiliary information set for certification is decrypted from the auxiliary information set for encryption certification by enciphering the 1st auxiliary information set for certification which is the usual auxiliary information set for certification (access ticket), creating the auxiliary information set for encryption certification, and carrying out the completely same processing as the usual authentication processing using the 2nd auxiliary information set for certification for accessing to this auxiliary information set for encryption certification.
[0043] Thus, by constituting, a use tariff creates a free ticket (1st auxiliary information set for certification), it enciphers, and implementation of the purchase function in prepaid one is made possible as a whole by constituting so that the ticket (2nd auxiliary information set for certification) for

decrypting the enciphered ticket may be published, the use tariff of this ticket (2nd auxiliary information set for certification) may be made into the charge and it may pay by prepaid one.
[0044] A RENTO function is realizable by indicating expiration date information to the use condition information on the 2nd auxiliary information set for certification in addition to this.
[0045] In addition, realizing efficiently is possible, without putting in an excessive program and data in an IC card with comparatively little capacity, since it constituted so that the same processing as authentication processing of the usual ticket might be performed in order to have decrypted the enciphered ticket.
[0046]
[Embodiment of the Invention] Hereafter, the example of this invention is explained.
[0047] Drawing 1 shows the block diagram of this example. In this example, prepaid information is held in certification data generation equipment, and the example (purchase) which purchases the access privilege of an application program is explained using that prepaid information.
[0048] Drawing 1 shows including the certification data verification equipment which verifies the certification data generated and outputted with certification data generation equipment.
[0049] First, after explaining the configuration of this example based on drawing 1 , while a flow chart shows the flow of processing of certification data verification equipment and certification data generation equipment, it explains. It explains to an example by carrying out authentication processing usual to explanation of the flow of processing, and the example pulled down from prepaid one for whenever [of one use to the use condition information L / every] is explained. And the example (purchase) which purchases the access privilege of an application program after explanation of the usual authentication processing is explained.
[0050] It is equipment of the pocket mold which [configuration of example] drawing 1 shows the configuration of an example as a whole, and a user holds certification data generation equipment 10 in this drawing, and had a count function in the interior like an IC card. The PC card which had a count function besides the IC card, a pocket mold information tool or a subnote PC, etc. may be used. It is desirable to be defended so that information on internal may not be simply altered from the outside.
[0051] A user is the personal computer which uses an application program, and certification data verification equipment 20 equips with and uses the IC card which is certification data generation equipment 10 for the slot of a personal computer.
[0052] Certification data verification equipment 20 consists of the data generation section 21 for authentication, and the certification data verification section 22 greatly. When needing to be attested, the data generation section 21 for authentication generates the data for authentication, and sends them to certification data generation equipment 10. The certification data with which the certification data verification section 22 was returned from certification data generation equipment 10 verify whether it is the right.
[0053] If it is protected by encryption etc. and a user is going to use an application program, an application program will restrict certification data-verification equipment 20, when the data for authentication corresponding to the application program are created, the certification data returned to certification data generation equipment 10 from delivery and certification data generation equipment 10 are verified and it is verified with the right, and will make it possible to remove and use protection of an application program.
[0054] On the other hand, certification data generation equipment 10 is constituted including the user proper information storage section 11, the frequency information attaching part 12, the access ticket storage section 13, the data input section 14 for authentication, the use conditional-judgment section 15, and the certification data generation output section 16.
[0055] The user proper information storage section 11 is a part holding a user's confidential information, and is different information for every user. As for user proper information, it is desirable to be constituted so that it may be enclosed when certification data generation equipment 10 is created, and it cannot take out to a user, either.
[0056] The frequency information attaching part 12 is a part holding prepaid information, and the

required frame is reduced according to use, purchase, etc. of an application program. Increasing is also possible when a frame decreases. The technique proposed by Japanese Patent Application No. No. 21373 [nine to] can be used for the approach of increase. By this technique, frequency information is increased using frequency information and the frequency information which signed. It is required to carry out the change in the frame in the frequency information attaching part 12 to insurance, and it is desirable to constitute so that access of those other than the defined approach cannot be performed.
[0057] The access ticket storage section 13 has memorized two or more access tickets. An access ticket gives a user access rating and is created by the ticket issue contractor who received commission from the application program implementer or the application program implementer. In this example, an access ticket is the group of the auxiliary information for certification and use condition information which were calculated by performing predetermined count to a user's proper information, the description information on access rating authentication, and the use condition information that described the access condition of access rating authentication. Although the access ticket storage section is constituted in the IC card, since only he who was published can use an access ticket, the copy is free and may consist of this examples in the IC card exterior.
[0058] The data input section 14 for authentication is a part which inputs the data for authentication sent from certification data verification equipment 20.
[0059] The use conditional-judgment section 15 takes out the access ticket corresponding to the inputted data for authentication from the access ticket storage section 13, and judges use conditions based on the use condition information in an access ticket. For example, it judges [whether the expiration date of an access ticket has run out or it is sufficient for paying a use tariff by prepaid one which it holds and] whether use conditions are judged and subsequent processings are continued.
[0060] The certification data generation output section 16 generates and outputs certification data, only when judged as continuation in the use conditional-judgment section 15. Certification data perform and create predetermined count to the auxiliary information for certification in the access ticket taken out in the use conditional-judgment section 15, the data for authentication, and a user's proper information.
[0061] Next, an example is given and it explains to a detail further. Explanation here makes the usual authentication processing an example, explains, and explains to the use condition information L the example pulled down from prepaid one for whenever [of one use / every].
[0062] Drawing 2 attaches a notation to the block diagram of drawing 1 . The notation corresponds with the following explanation.
[0063] below the [usual authentication processing] -- law -- the example using the RSA (Rivest-Shamir-Adelman) code in n is explained to a detail. First, the usual authentication processing is explained. In the following examples, the software vendor which is the implementer of an application program explains the example which performs all from issue of an IC card to issue of a ticket. In this example, the software vendor knows all users' confidential information du. The configuration whose ticket issue contractor performs issue of an IC card and a ticket besides this is also possible.
[0064] A software vendor creates the cryptographic key to an application program to protect. since RSA cryptograph is used here -- the big prime factors p and q -- secret -- creating -- law -- a number n is created as n=p-q. next, law -- the origin of a number n -- a cryptographic key E and the decode key D --
[0065]
[Equation 1] ED**1 mod phi (n)
******** -- it generates like. phi (n) is the Euler number and is phi(n) = (p-1) (q-1) here.
[0066] Next, a software vendor enciphers a part or all of an application program that wants to make and protect the common cryptographic key K by K, and is [0067].
[Equation 2] K'=KE mod n is calculated, and it embeds and distributes to the application program which enciphered K' so that the 3rd person cannot take out.
[0068] The user who wants to use this application program will receive the access ticket corresponding to this beforehand.
[0069] A software vendor publishes an access ticket in response to the access ticket issue demand from a user. A software vendor picks out the confidential information du of the user who required, and the

decode key (D, n) corresponding to the cryptographic key (E, n) used on the occasion of encryption of an application program from a database. Next, the use condition information L given to an access ticket is created. Here, since it pulls down from prepaid one and charges, the amount of use pulled down about one use is set to L. And such information is used and it is [0070].
[Equation 3] t=D-F(n,L,du)
It carries out and the auxiliary information t for certification is created. On the other hand, function F() is the function of tropism, and, on the other hand, can use tropism Hash Function MD5, SHA, etc. a common key encryptosystem DES (DataEncryption Standard), etc. here.
[0071] A software vendor is published to a user by using the group of (t, L, n) as an access ticket.
[0072] If a user is going to use an application program, certification data verification equipment will create the data for authentication corresponding to the application program (C, n), and will send them to certification data generation equipment.
[0073] The flow of this processing is shown in the flow chart of drawing 3 , and it explains based on this.
: (Step S11) The certification data generation section 21 takes out K' and n from the protected application program.
: (Step S12) The certification data generation section generates a random number r, and stores it in a random-number attaching part.
(Step S13) :C=rEK' mod n is calculated.
(Step S14) It sends to certification data generation equipment 10 by using the group of : (C, n) as the data for authentication.
[0074] Next, the flow of certification data generation equipment 10 is shown in drawing 4 , and processing of certification data generation equipment 10 is explained based on this.
: (Step S21) The data for authentication (C, n) are inputted from the data input section 14 for authentication.
: (Step S22) The use conditional-judgment section 15 uses n as a key, searches the access ticket storage section, and takes out an access ticket (t, L, n).
: (Step S23) The use conditional-judgment section 15 compares the frequency information V on the use conditions L in the taken-out access ticket (amount of use), and a frequency information attaching part.
: (Steps S24-S25) At the time of V>=L, the certification data generation output section 16 progresses to (step S26). When that is not right, the certification data generation output section outputs an error, and is completed.
: (Step S26) Only the part of the use conditions (amount of use) L reduces the frequency information V for which the use conditional-judgment section 15 is held at the frequency information attaching part 12.

: (Steps S26-S29) The certification data generation output section 16 calculates and outputs the certification data R using the auxiliary information t for certification which the use conditional-judgment section 15 took out, the use conditions L (amount of use), and du read from the user proper information storage section 11.
[0075]
[Equation 4] R'=CF (n, L, du) mod nR=CtR' mod In n drawing 4 , although the certification data R are calculated, count of R' is once divided. In order for this to use a user's confidential information for count of R', it is necessary to calculate but so that the processing may not leak outside, and once count of R' finishes, it will be for performing count of R externally. Thus, you may calculate by dividing into R' and R, and it does not matter even if it calculates at once.
[0076] Next, processing of the certification data verification section of certification data verification equipment 20 is explained. The certification data R outputted from certification data generation equipment 10 are [the right user proper information du and] [0077] when calculated using a right access ticket (the auxiliary information t for right certification, the right use conditions L).
[Equation 5]
R=CtR' mod n=CD-F(n, L, du) CF(n, L, du) mod n=CD mod n=(rE K') D mod n=(rEKE) D mod n=(rK)

ED mod It becomes n=rK.
[0078] Then, in the certification data verification section 22, a random number r is taken out from the random-number attaching part 23, and it is [0079].
[Equation 6] r-1R mod By calculating n, the common cryptographic key K which had enciphered application can come to hand. Certification data verification equipment can decode the part as which application was enciphered by this common cryptographic key K, and can perform application.
[0080] In this example, certification data verification equipment has that application has performed correctly, and it is judged that verification was completed correctly.
[0081] Explanation of the usual authentication processing is ended above.
[0082] The example (purchase) which purchases the access privilege of an application program is explained using a [purchase], next prepaid information.
[0083] In order to realize this function, the 1st access ticket is decrypted from an encryption access ticket by enciphering the 1st access ticket which is the usual access ticket, creating the encryption access ticket, and performing the completely same processing as the usual authentication processing using the 2nd access ticket for accessing to this encryption access ticket.
[0084] And at this time, a use tariff creates the 1st access ticket as a free ticket, and the 2nd access ticket is constituting so that a use tariff's may be made into the charge and it may pay by prepaid one, and enables implementation of the purchase function in prepaid one as a whole.
[0085] First, the application program which wants to realize the function of a purchase is set to AP1. AP1 is protected like above-mentioned explanation.
[0086] A <explanation of protection of application program AP 1> software vendor creates the cryptographic key to an application program to protect. since RSA cryptograph is used here -- the big prime factors p1 and q1 -- secret -- creating -- law -- an n1 number is created as n1=p1 and q1. next, law -- the origin of an n1 number -- a cryptographic key E1 and the decode key D1 -- [0087]
[Equation 7] E1 and D 1**1 mod phi (n1)
******** -- it generates like. phi (n1) is the Euler number and is phi(n1) = (p1-1) (q1-1) here.
[0088] Next, a software vendor enciphers a part or all of an application program that wants to make and protect the common cryptographic key K1 by K1, enciphers the common cryptographic key K1 by the cryptographic key E1 according to the following formulas further, and generates K1'.
[0089]
[Equation 8] It embeds and distributes to the application program which enciphered K1'=K1E1 mod n1 and K1' so that the 3rd person cannot take out easily. Moreover, n1 is embedded at the enciphered application program.
[0090] A software vendor memorizes the group created (n1, D1, phi (n1)) in an access ticket information database.
[0091] Next, creation of a prepaid payment purchase ticket is explained. Drawing 5 shows the example of a configuration of the auxiliary information generation equipment 30 for certification. In this example, a prepaid payment purchase ticket is outputted by considering the 1st use condition information, the 1st decode key, user proper information, and 2nd use condition information as an input. In drawing 5 , the input section 31 is a part which inputs the 1st use condition information, the 1st decode key, user proper information, and the 2nd use condition information. The 1st decode key storage section 33 is a part which memorizes the 1st decode key inputted from the input section 31. The 1st decode key is a decode key (D1, n1) corresponding to the cryptographic key (E1, n1) which enciphered the common cryptographic key K1 used for encryption of an application program AP 1.
[0092] The user proper information storage section 34 is a part which memorizes the user proper information that it was inputted from the input section 31. This is the same as that of what is stored in a user's certification data generation equipment 10.
[0093] When a user requests issue of a ticket, a user's identification information U and a user send n1 taken out from the application program AP 1 which wishes to use to a software vendor. A software vendor from the User Information database which matches and holds a user's identification information U and user proper information du User proper information is acquired by retrieving the user proper

information du corresponding to a user's identification information U. From the access ticket information database holding a group, the decode key (D1, n1) corresponding to n1 is obtained, and moreover (n, D, phi (n)) inputs into the auxiliary information generation equipment 30 for certification.
[0094] The 1st use condition information storage section 32 and the 2nd use condition information storage section 35 are parts which memorize the 1st use condition information and the 2nd use condition information, respectively. The 1st use condition information describes the use conditions of an application program AP 1, and the 2nd use condition information describes the use conditions of a prepaid payment purchase ticket. In the case of the prepaid payment purchase ticket, since it is charged at the 1st utilization time and has the property of not being charged in the utilization time of the 2nd henceforth, the information meaning being no charge at least is included in the 1st use condition information, and the information meaning being a charge at least is included at the 2nd use condition information.
[0095] The 1st ticket generation section 36 is a part which performs predetermined count to the 1st use condition information and the 1st decode key which were inputted, and user proper information, and generates an access ticket.
[0096] The component 41 which consists of the 1st use condition information storage section 32, the 1st decode key storage section 33, the user proper information storage section 34, and the 1st ticket generation section 36 is making the configuration same with generating the usual access ticket.
[0097] The 2nd key generation section 37 is a part which generates the key for enciphering the 1st access ticket generated in the 1st ticket generation section 36.
[0098] The encryption section 38 is a part which enciphers the 1st access ticket generated in the 1st ticket generation section 36 using the encryption key generated in the 2nd key generation section 37.
[0099] The 2nd ticket generation section 39 is a part which generates the 2nd access ticket which is needed in order to decrypt the encryption access ticket enciphered in the encryption section 38.
[0100] The ticket output section 40 is outputted as a prepaid payment purchase ticket combining the encryption access ticket enciphered in the encryption section 38, and the 2nd access ticket generated in the 2nd ticket generation section 39.
[0101] The approach of creation of a prepaid payment purchase ticket is explained below to <creation of a prepaid payment purchase ticket> using the flow chart of drawing 6 .
[0102] A software vendor publishes a prepaid payment purchase ticket in response to the prepaid payment purchase ticket issue demand from a user. The user who requests issue of a ticket sends n1 taken out from the application program AP 1 with which a user's identification information U and a user wish to use to a software vendor.
[0103] : (Step S31) A software vendor inputs the group (U, n1) of n1 taken out from identification information U and application program AP 1 of the user who is the prepaid payment purchase ticket issue demand from a user. Moreover, the 1st use condition information L1 which described the use conditions of an application program AP 1, and the 2nd use condition information L2 which described the use conditions of a prepaid payment purchase ticket are also inputted. Here, it is [0104] as which the 1st use condition information L1 means that a use tariff is no charge since it aims at generation of a prepaid payment purchase ticket.
[Equation 9] It is [0105] as which it is L1=0 and the 2nd use condition information L2 means that the tariff of a purchase is a charge.
[Equation 10] It is referred to as L2=A. However, A is figures other than zero, for example, is 100.
[0106] : (Step S32) The user proper information du corresponding to a user's identification information U is retrieved from the User Information database which matches and holds a user's identification information U and user proper information du.
(Step S33) From the access ticket information database holding the group of : (n, D, phi (n)), the 1st decode key (D1, n1) corresponding to n1 is searched.
: (Step S34) The 1st access ticket T1 for a user to access AP1 is created.
[0107]
[Equation 11] T1=(t1,L1,n1)

t1=D1-F(n1,L1,du)
(Step S35) : -- in order to encipher the 1st access ticket T1 -- the 2nd law -- an n2 number, the 2nd cryptographic key E2, and the 2nd decode key D2 are generated. the big prime factors p2 and q2 are generated, and the following formulas are realized -- as -- law -- an n2 number, a cryptographic key E2, and the decode key D2 are generated.
[0108]
[Equation 12] n2=p2, q2E2, and D 2**1 mod phi (n2)
phi(n2) = (p2-1) (q2-1)
: (Step S36) The 1st access ticket T1 is enciphered by the 2nd generated cryptographic key E2. What enciphered T1 is made into T1'.
[0109]
[Equation 13] T1'=T1E2 mod n2 (step S37): Create the 2nd access ticket T2 for a user to decode enciphered access ticket T1'.
[0110]
[Equation 14] T2=(t2,L2,n2)
t2=D2-F(n2,L2,du)
(Step S38) : (T1', n2) (T2) is made into a group, and it outputs as a prepaid payment purchase ticket.
[0111] A software vendor sends the outputted prepaid payment purchase ticket (T1', n2) (T2) to a user.
[0112] Next, the example of use of a prepaid payment purchase ticket is explained.
[0113] The user who received the (example a) prepaid payment purchase ticket (T1', n2) (T2) stores T2 in the access ticket storage section 13 first. [<example of use of prepaid payment purchase ticket>]
(b) Next, input from the data input section 14 for authentication of the certification data generation equipment 10 with which he holds (T1', n2).
[0114] Hereafter, processing in certification data generation equipment 10 is performed according to drawing 4 . Now, suppose at the frequency information attaching part 12 of certification data generation equipment 14 that the prepaid information V on 800 frequencies is held. (V=800)
: (Step S21) From the data input section 14 for authentication, the data for authentication (T1', n2) are inputted.
: (Step S22) The use conditional-judgment section 15 uses n2 as a key, searches the access ticket storage section 13, and takes out access ticket T2= (t2, L2, n2).
: (Step S23) The use conditional-judgment section 15 compares the frequency information V on the frequency information attaching part 12 with the use conditions L2 in the taken-out access ticket.
: (Step S24) Since it is now, L2=100, and V= 800, it is [0115].
[Equation 15] V>=L2 is realized and it progresses to (step S26).
: (Step S26) Only the part of the use conditions L2 reduces the frequency information V for which the use conditional-judgment section 15 is held at the frequency information attaching part 12.
[0116]
[Equation 16] As an acquisition tariff of a prepaid payment purchase ticket, V=800-100=700 [V], i.e., frequency information, are pulled down the number of 100 degrees, and it serves as remainder 700 frequency.
: (Steps S27-S29) The certification data generation output section 16 calculates and outputs the certification data R using the auxiliary information t2 for certification and the use conditions L2 which the use conditional-judgment section 15 took out, and du read from the user proper information storage section 11.
[0117]
[Equation 17] R'=T1'F (n2, L2, du) mod n2R=T1't2R' mod It is [0118] when n2R is calculated.
[Equation 18]
R=T1't2R' mod n2=T1'D2-F(n2, L2, du) CF(n2, L2, du) mod n2=T1' D2 mod n2=(T1 E2) D2 mod Count called n2=T1 is realized and it is [0119] as certification data R from the certification data generation output section 16.
[Equation 19] R=T1 is outputted.

[0120] That is, if it inputs from the data input section 14 for authentication of the certification data generation equipment 10 with which he holds (T1', n2), L2 will be pulled down from the frequency information V, and T1 by which T1' was decoded as a result will be outputted.
[0121] (c) A user stores T1 which came to hand in the access ticket storage section 13.
[0122] (d) Since the user obtained the access ticket T1 for using an application program AP 1, he uses an application program AP 1.
[0123] Hereafter, data generation processing for authentication in certification data verification equipment 10 is performed according to drawing 3 .
: (Step S11) The data generation section 21 for authentication takes out K1' and n1 from the protected application program.
: (Step S12) The data generation section 21 for authentication generates a random number r, and stores it in the random-number attaching part 23.
(Step S13) :C=rEK1' mod n1 is calculated.
(Step S14) It sends to certification data generation equipment 10 by using the group of : (C, n1) as the data for authentication.
(e) Processing in certification data generation equipment 10 is again performed according to drawing 4 .
: (Step S21) From the data input section 14 for authentication, the data for authentication (C, n1) are inputted.
: (Step S22) The use conditional-judgment section 15 uses n1 as a key, searches the access ticket storage section 13, and takes out access ticket T1= (t1, L1, n1).
: (Step S23) The use conditional-judgment section 15 compares the frequency information V on the frequency information attaching part 12 with the use conditions L1 in the taken-out access ticket.
: (Step S24) Since it is now, L1=0, and V= 700, it is [0124].
[Equation 20] V>=L1 is realized and it progresses to (step S26).
: (Step S26) Only the part of the use conditions L1 reduces the frequency information V for which the use conditional-judgment section 15 is held at the frequency information attaching part 12.
[0125]
[Equation 21] First, as an acquisition tariff of a prepaid payment purchase ticket, since V=700-0=700 [V], i.e., frequency information, are pulled down the number of 100 degrees, by use of the 2nd henceforth, it is not pulled down but serves as as [remainder 700 frequency].
: (Steps S27-S29) The certification data generation output section 16 calculates and outputs the certification data R using the auxiliary information t1 for certification and the use conditions L1 which the use conditional-judgment section 15 took out, and du read from the user proper information storage section 11.
[0126]
[Equation 22] R'=CF(n1, L1, du) mod n1R=Ct1R' mod n1, i.e., [0127]
[Equation 23]
R=Ct1R' mod The certification data verification section 22 of n1=rK(f) certification data verification equipment 20 processes like the usual authentication, takes out a random number r from the random-number attaching part 23, and is [0128].
[Equation 24] r-1R mod By calculating n1, the common cryptographic key K which had enciphered application can come to hand. Certification data verification equipment can decode the part as which application was enciphered by this common cryptographic key K, and can perform application.
[0129] After this, even if it performs an application program AP 1 what times, same processing is performed and it can use for free.
[0130] As explained above, what (purchase) the access privilege of an application program is purchased for with constituting as mentioned above using prepaid information becomes possible.
[0131] In the above, implementation of the purchase function in prepaid one was explained.
[0132] When certification data generation equipment is equipped with a clock, and in addition to the information of no charge the amount of use indicates expiration date information and compares with time of day in the use condition information L on the 1st access ticket at every use of the 1st access

ticket besides this, it is also possible to realize the RENTO function in prepaid one.
[0133] Furthermore, it is possible to limit the term which distributes the 1st access ticket (defrosting) etc. by equipping certification data generation equipment with a clock, and comparing with time of day as another example, in the case of decode of the 1st access ticket which indicated expiration date information in the use condition information L on the 2nd access ticket, and was enciphered.
[0134] Moreover, although this example explained by carrying out based on RSA cryptograph, not only this but other cipher systems may be used. Moreover, the implementation type of an access ticket is not restricted to this, either.
[0135]

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the block diagram showing the configuration of the example of this invention.
[Drawing 2] It is drawing which explains the configuration of drawing 1 to a detail.
[Drawing 3] It is a flow chart explaining the data generation processing for authentication of the certification data verification equipment of drawing 1 .
[Drawing 4] It is a flow chart explaining certification data generation processing of the certification data generation equipment of drawing 1 .
[Drawing 5] It is the block diagram showing the auxiliary information generation equipment for certification which generates the ticket used for generation of the certification data of drawing 1 .
[Drawing 6] It is drawing explaining generation of the ticket used for generation of the certification data of drawing 1 .
[Description of Notations]
10 Certification Data Generation Equipment
11 User Proper Information Storage Section
12 Frequency Information Attaching Part
13 Access Ticket Storage Section
14 Data Input Section for Authentication
15 Use Conditional-Judgment Section
16 Certification Data Generation Output Section
20 Certification Data Verification Equipment
21 Data Generation Section for Authentication
22 Certification Data Verification Section
23 Random-Number Attaching Part
30 Auxiliary Information Generation Equipment for Certification
32 1st Use Condition Information Storage Section
33 1st Decode Key Storage Section
34 User Proper Information Storage Section
35 2nd Use Condition Storage Section
36 1st Ticket Generation Section
37 2nd Key Generation Section
38 Encryption Section
39 2nd Ticket Generation Section
40 Ticket Output Section

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－32037

(43)公開日　平成11年(1999)２月２日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｂ
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ	9/06	５５０Ｚ
	15/00	３３０		15/00	３３０Ｂ
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｂ
					６４０Ｅ

審査請求　未請求　請求項の数11　ＯＬ　（全 18 頁）

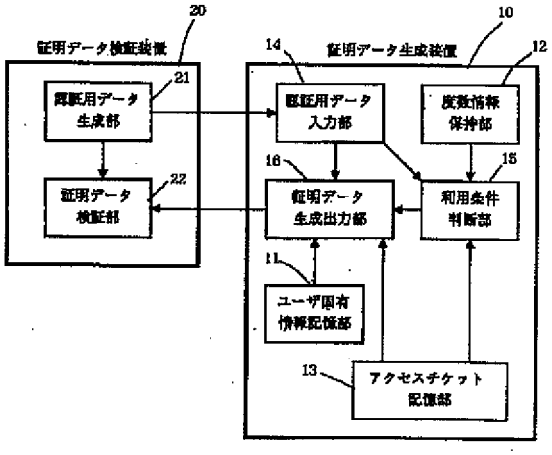
(21)出願番号　特願平9－188801

(22)出願日　平成９年(1997)７月14日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号
(72)発明者　中垣　寿平
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内
(72)発明者　申　吉浩
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内
(74)代理人　弁理士　澤田　俊夫

(54)【発明の名称】　証明データ生成装置

(57)【要約】
【課題】　証明データ生成装置側に余分な負荷をかけることなく、買い取りやレントのアクセス資格をプリペイドで支払う。
【解決手段】　プリペイド払いパーチェス・チケットのT_2はアクセスチケット記憶部１３に格納される。次に、（T_1'，n_2）が認証用データ入力部１４に入力される。利用条件判断部１５は、対応するアクセスチケット（t_2，L_2，n_2）を取り出し、利用条件L_2が満たされるか調べ、満たされれば、度数情報Ｖを減額する。証明データ生成出力部１６は、利用条件判断部１５が取り出した証明用補助情報t_2、利用条件L_2と、ユーザ固有情報記憶部１１から読み出したｄｕとを用いて証明データＲを計算してT_1を出力する。ユーザはT_1を用いて買い取り状態であるいはレント状態でプログラムへのアクセスを行う。



実施例の構成図

1

【特許請求の範囲】

【請求項１】　ユーザのアクセス資格を認証するために生成され、正当性を検証される証明データを生成する証明データ生成装置において、

認証用データを入力する認証用データ入力手段と、

ユーザの固有情報を記憶するユーザ固有情報記憶手段と、

ユーザの固有情報と、アクセス資格認証の特徴情報と、アクセス条件を記述した利用条件情報とに対し、所定の計算を実行して生成した証明用補助情報と、利用条件情報との組を含む証明用補助情報セットを記憶する証明用補助情報セット記憶手段と、

入力された認証用データに対応する証明用補助情報セットを上記証明用補助情報セット記憶手段から取り出し、上記取り出した証明用補助情報セットの利用条件情報に従い、以降の処理を継続するかどうかの判断を行う利用条件判断手段と上記利用条件判断手段において継続と判断されたときに、上記取り出した証明用補助情報セットと、上記認証用データ入力手段から入力された認証用データと、上記ユーザ固有情報記憶手段に記憶されている上記ユーザの固有情報とに所定の計算を施して証明データを生成し出力する証明データ生成出力手段とを有し、

上記認証用データ入力手段から、第１の証明用補助情報セットを暗号関数における暗号化鍵で暗号化した暗号化証明用補助情報セットを入力し、

上記利用条件判断手段は、上記証明用補助情報セット記憶手段から、入力された暗号化証明用補助情報セットに対応する第２の証明用補助情報セットを取り出し、上記取り出した第２の証明用補助情報セットの利用条件情報に従い、所定の処理を行った後、以降の処理を継続するかどうかの判断を行い、

上記証明データ生成出力手段は、上記処理を行うことにより、上記暗号化証明用補助情報セットを復号化した結果である第１の証明用補助情報セットを出力することを特徴とする証明データ生成装置。

【請求項２】　少なくとも、上記ユーザ固有情報記憶手段と、上記利用条件判断手段と、上記証明データ生成出力手段とが、内部のデータおよび処理手続きを外部から観測することを困難ならしめる防御手段中に保持されている請求項１記載の証明データ生成装置。

【請求項３】　さらに電子度数情報を保持する度数情報保持手段を備え、上記利用条件情報には、利用したときに支払うべき利用度数を含み、上記利用条件判断手段は、上記度数情報保持手段に保持されている電子度数情報と、上記利用条件情報に含まれる利用度数とを比較して、上記度数情報保持手段に保持されている電子度数情報が利用条件情報に含まれる利用度数以上の時にのみ、上記度数情報保持手段に保持されている電子度数情報から上記利用条件情報に含まれる利用度数分の度数を減額して、以降の処理を継続するという判断を行う請求項１または２記載の証明データ生成装置。

2

【請求項４】　上記第１の証明用補助情報セットに含まれる第１の利用条件情報に含まれる利用度数は０度数であり、上記第２の証明用補助情報セットに含まれる第２の利用条件情報に含まれる利用度数は０以外であることを特徴とする請求項３記載の証明データ生成装置。

【請求項５】　さらに時刻を示す時計を備え、上記第１の証明用補助情報セットに含まれる第１の利用条件情報には、さらに有効期限情報が記載され、上記利用条件判断手段は、上記時刻と上記有効期限情報とを比較し、該時刻が有効期限内にある時にのみ、以降の処理を継続するという判断を行う請求項１、２、３または４記載の証明データ生成装置。

【請求項６】　少なくとも、上記証明用補助情報セット記憶手段以外の手段が、携帯可能な小型演算装置として構成されている請求項１、２、３、４または５記載の証明データ生成装置。

【請求項７】　ユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証装置において、

認証用データを記憶する第１の記憶手段と、

ユーザの固有情報を記憶する第２の記憶手段と、

上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対して所定の計算を実行して生成した第１の証明用補助情報を暗号化して生成した暗号化証明用補助情報を記憶する第３の記憶手段と、

上記ユーザの固有情報と、上記暗号化の復号鍵と、アクセス条件を記述した利用条件情報とに対して、所定の計算を実行して生成した第２の証明用補助情報と、上記利用条件情報とからなる第２の証明用補助情報セットを記憶する第４の記憶手段と、

上記第４の記憶手段に記憶されている上記第２の証明用補助情報セットに含まれる上記利用条件情報にしたがって所定の処理を継続するかどうかを判断する手段と、

上記所定の処理を継続すると判断したときに、上記第３の記憶手段に記憶されている上記暗号化証明用補助情報と、上記第２の記憶手段に記憶されている上記ユーザの固有情報と、上記第４の記憶手段に記憶されている上記第２の証明用補助情報セットとに対して所定の計算を実行して上記第１の証明用補助情報を復元する手段と、

上記第１の記憶手段に記憶されている上記認証用データと、上記第２の記憶手段に記憶されている上記ユーザの固有情報と、復元した上記第１の認証用補助情報とに対して所定の計算を実行して証明データを生成する手段と、

生成された上記証明データを検証する手段とを有することを特徴とするアクセス資格認証装置。

【請求項８】　ユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上

記ユーザのアクセス資格を認証するアクセス資格認証装置において、
認証用データを記憶する第１の記憶手段と、
ユーザの固有情報を記憶する第２の記憶手段と、
上記ユーザの固有情報と、アクセス資格認証の特徴情報と、アクセス条件を記述した第１の利用条件情報とに対し、所定の計算を実行して生成した第１の証明用補助情報と、上記第１の利用条件情報とからなる第１の証明用補助情報セットを暗号化して生成した暗号化証明用補助情報セットを記憶する第３の記憶手段と、
上記ユーザの固有情報と、上記暗号化の復号鍵と、アクセス条件を記述した第２の利用条件情報とに対して、所定の計算を実行して生成した第２の証明用補助情報と、上記第２の利用条件情報とからなる第２の証明用補助情報セットを記憶する第４の記憶手段と、
上記第４の記憶手段に記憶されている上記第２の証明用補助情報セットに含まれる上記第２の利用条件情報にしたがって第１の処理を継続するかどうかを判断する手段と、
上記第１の処理を継続すると判断したときに、上記第３の記憶手段に記憶されている上記暗号化証明用補助情報セットと、上記第２の記憶手段に記憶されている上記ユーザの固有情報と、上記第４の記憶手段に記憶されている上記第２の証明用補助情報セットとに対して所定の計算を実行して上記第１の証明用補助情報セットを復元する手段と、
復元された上記第１の証明用補助情報セットに含まれる上記第１の利用条件情報にしたがって第２の処理を継続するかどうかを判断する手段と、
上記第２の処理を継続すると判断したときに、上記第１の記憶手段に記憶されている上記認証用データと、上記第２の記憶手段に記憶されている上記ユーザの固有情報と、復元した上記第１の証明用補助情報セットとに対して所定の計算を実行して証明データを生成する手段と、
生成された上記証明データを検証する手段とを有することを特徴とするアクセス資格認証装置。
【請求項９】　ユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証方法において、
認証用データを記憶する第１のステップと、
ユーザの固有情報を記憶する第２の記憶ステップと、
上記ユーザの固有情報と、アクセス資格認証の特徴情報と、アクセス条件を記述した第１の利用条件情報とに対し、所定の計算を実行して生成した第１の証明用補助情報と、上記第１の利用条件情報とからなる第１の証明用補助情報セットを暗号化して生成した暗号化証明用補助情報セットを記憶する第３のステップと、
上記ユーザの固有情報と、上記暗号化の復号鍵と、アクセス条件を記述した第２の利用条件情報とに対して、所定の計算を実行して生成した第２の証明用補助情報と、上記第２の利用条件情報とからなる第２の証明用補助情報セットを記憶する第４の記憶ステップと、
上記第４の記憶ステップで記憶された上記第２の証明用補助情報セットに含まれる上記第２の利用条件情報にしたがって第１の処理を継続するかどうかを判断するステップと、
上記第１の処理を継続すると判断したときに、上記第３の記憶ステップで記憶された上記暗号化証明用補助情報セットと、上記第１の記憶ステップで記憶された上記ユーザの固有情報と、上記第４の記憶ステップで記憶された上記第２の証明用補助情報セットとに対して所定の計算を実行して上記第１の証明用補助情報セットを復元するステップと、
復元された上記第１の証明用補助情報セットに含まれる上記第１の利用条件情報にしたがって第２の処理を継続するかどうかを判断するステップと、
上記第２の処理を継続すると判断したときに、上記第１の記憶ステップで記憶された上記認証用データと、上記第２の記憶ステップで記憶された上記ユーザの固有情報と、復元した上記第１の証明用補助情報セットとに対して所定の計算を実行して証明データを生成するステップと、
生成された上記証明データを検証するステップとを有することを特徴とするアクセス資格認証方法。
【請求項１０】　ユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証装置に用いる証明用補助情報を生成する証明用補助情報生成装置において、
ユーザの固有情報と、アクセス資格認証の特徴情報と、アクセス条件を記述した第１の利用条件情報とに対し、所定の計算を実行して第１の証明用補助情報を生成する手段と、
上記第１の証明用補助情報と、上記第１の利用条件情報とからなる第１の証明用補助情報セットを暗号化する手段と、
上記ユーザの固有情報と、上記暗号化の復号鍵と、アクセス条件を記述した第２の利用条件情報とに対して、所定の計算を実行して第２の証明用補助情報を生成する手段と、
上記暗号化した第１の証明用補助情報セットと上記第２の証明用補助情報セットとから複合的な証明用補助情報を生成して出力する手段とを有することを特徴とする証明用補助情報生成装置。
【請求項１１】　ユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証装置に用いる証明用補助情報を生成する証明用補助情報生成方法において、

ユーザの固有情報と、アクセス資格認証の特徴情報と、アクセス条件を記述した第１の利用条件情報とに対し、所定の計算を実行して第１の証明用補助情報を生成するステップと、
上記第１の証明用補助情報と、上記第１の利用条件情報とからなる第１の証明用補助情報セットを暗号化するステップと、
上記ユーザの固有情報と、上記暗号化の復号鍵と、アクセス条件を記述した第２の利用条件情報とに対して、所定の計算を実行して第２の証明用補助情報を生成するステップとを有することを特徴とする証明用補助情報生成方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ユーザの権限を証明するために生成された証明データの正当性を検証することによりユーザのアクセス資格を認証する技術に関し、とくに上記証明データを生成する証明データ生成装置に関するものである。

【０００２】

【従来の技術】本発明と同分野に属する先行技術としてプログラムの実行制御技術が知られている。プログラム実行制御技術は、
①アプリケーションプログラム中にユーザ認証のためのルーチンを埋め込み、②該ルーチンはアプリケーションの実行を試みているユーザが正規の認証用の鍵を保有していることを検査し、
③前記認証用の鍵の存在が確認された場合に限りプログラムを続行し、それ以外の場合にはプログラムの実行を停止する技術である。

【０００３】このような技術を利用することにより、認証鍵を保有する正規のユーザにのみアプリケーションプログラムの実行を可能ならしめることが出来る。当技術はソフトウェア頒布事業において実用化されており、製品として、例えばＲａｉｎｂｏｗ　Ｔｅｃｈｎｏｌｏｇｉｅｓ，Ｉｎｃ．社のＳｅｎｔｉｎｅｌＳｕｐｅｒＰｒｏ（商標）や、Ａｌａｄｄｉｎ　Ｋｎｏｗｌｅｄｇｅ　Ｓｙｓｔｅｍｓ　Ｌｔｄ．社のＨＡＳＰ（商標）等がある。

【０００４】これらの技術では、ユーザの認証鍵は、ソフトウェアベンダが、複製を防ぐためにハードウェア中のメモリに厳重に封入し、郵便などの物理的手段を用いてユーザに配布し、ユーザはこれを所有のパソコンなどに装着して利用する。

【０００５】これらの技術は、アプリケーションプログラムを作成する際に、プログラム作成者がユーザが持つ認証鍵を予め想定した上で、該認証鍵に基づいてプログラムの保護処理を行わなければならない。つまり、プログラム作成者は、鍵内蔵ハードウェアからの正しい返信をプログラム作成時に予測して、正しい返信を受けた場合にのみプログラムが正常に動作するようにプログラムの作成を行わなければならない。

【０００６】このような特徴を有する従来技術の利用形態は、基本的に以下の２通りとなる。

【０００７】①第１の方法では、ユーザの認証鍵をユーザ毎に異なるように用意する。即ち、ユーザ甲には認証鍵甲、ユーザ乙には認証鍵乙というように、ユーザ毎に異なる認証鍵を一つずつ用意する。

【０００８】②第２の方法では、プログラム作成者はアプリケーション毎にそれぞれ異なる認証鍵を用意する。即ち、アプリケーション甲には認証鍵甲、アプリケーション乙には認証鍵乙というように、アプリケーション毎に異なる認証鍵を一つずつ用意し、固有の認証鍵を識別するように各アプリケーションプログラムを作成する。

【０００９】しかし、これらのいずれの場合にも、以下に述べるような問題を有する。

【００１０】第１の方法の場合、プログラム作成者は、プログラム中の認証ルーチンをユーザ毎に適切に変えてプログラムを作成する必要がある。つまり、ユーザ毎に認証鍵が異なるので、プログラム中の認証ルーチンは該プログラムを利用するユーザ固有の認証鍵を識別するように作成されなければならず、プログラム作成者は利用ユーザの数だけ異なるプログラムを作成する必要がある。

【００１１】対象となるユーザが多数の場合、プログラムをユーザ毎に個別化する作業はプログラム作成者にとって耐えがたい労力を要求し、管理しなければならないユーザ認証鍵のリストも膨大なものとなる。

【００１２】第２の方法の場合、第１の方法の場合のようにユーザ毎にプログラムを個別的に作成する必要は無くなるが、逆に、ユーザは利用するアプリケーションの数だけ認証鍵を保持しなければならないこととなる。

【００１３】この制約はプログラム作成者及びユーザそれぞれに以下のような問題を惹起する。

【００１４】前述のように、認証鍵はハードウェアに厳重に封入した状態でユーザに配布する必要がある。従って、プログラム自身はネットワークを介して簡便に配布することができるのと対照的に、認証鍵を内蔵するハードウェアの配布は郵便等の物理手段に頼らざるを得ない。この制限は、コスト、時間、梱包の手間いずれをとっても、プログラム作成者とって大きな負担となる。

【００１５】プログラム作成者は、ユーザの要求に応えるべく、アプリケーション毎に異なるハードウェアを一定個数ストックしておかなければならず、在庫管理のコストを必要とする。

【００１６】また、ユーザは利用するアプリケーションを変更する度にハードウェアを交換しなければならないという煩雑さに甘んじなければならない。

【００１７】ユーザがあるアプリケーションを使いたいとしても、認証鍵が封入されたハードウェアが届くまで

待たねばならず、即座に利用できないという点での不便さも生ずる。

【００１８】この問題を解決する技術として、本出願人は新たなアクセス資格検証手法を提案している（特願平０８－０６２０７６号、現在未公開）。

【００１９】特願平０８－０６２０７６号の提案では、証明用補助情報（アクセスチケット）を導入することにより、アクセス資格認証の特徴情報とユーザ固有情報とを独立させ、プロテクト側も、ユーザ側も１つの固有情報を準備しておけばすむようにしている。

【００２０】アクセスチケットは、特定のユーザの固有情報とアクセス資格認証の特徴情報とに基づいて計算されるデータであり、また、ユーザ固有情報を知らずに、アクセスチケットからアクセス資格認証の特徴情報を計算することは困難である。そして、ユーザ固有情報とアクセスチケットとの正しい組み合わせ、すなわち、ユーザ固有情報と該ユーザ固有情報に基づいて計算されたアクセスチケットの組み合わせが入力された場合に限って、正しい証明用データが計算される。

【００２１】したがってユーザはあらかじめ固有情報を保持し、プログラム作成者等のプロテクト者はユーザが所持する固有情報とは独立にアクセス資格認証の特徴情報を用意し、アクセスチケットをユーザの固有情報とアプリケーションプログラムの作成等に使用したアクセス資格認証の特徴情報とに応じて作成し、配布することにより、実行制御等のユーザのアクセス資格の認証を行う事ができる。

【００２２】この技術を用いて、アプリケーションプログラムにプロテクトを行ってユーザに配布し、アプリケーションプログラムの利用を希望するユーザに、アクセスチケットを提供するサービスが考えられる。

【００２３】希望するユーザに、ユーザ毎に異なる固有情報を封入したＩＣカードなどの媒体を渡しておき、またプログラム作成者はアクセス資格認証の特徴情報を用いてプログラムにプロテクトをかけて配布し、プログラムの利用を希望するユーザに、プログラム作成者またはプログラム作成者から委託を受けたチケット発行業者がアクセスチケットを提供する。

【００２４】このようなサービスを考えた場合、いつどのようにして課金するかということが問題になる。この例の場合では、アクセスチケットを発行する際に、チケットの発行と引換えにプログラムの代金に相当する料金を徴収することができる。

【００２５】ところで、このようなプログラムの利用権の売買サービスを考える場合、以下のような権利の形態が考えられる。

①パーチェス（ｐｕｒｃｈａｓｅ）：利用権を買いとってしまう方法。一度購入すると、永久に利用することができる。その後、利用する、しないにかかわらず、料金は同じである。

②ペイ・パー・ユース（ｐａｙ－ｐｅｒ－ｕｓｅ）：利用量課金とも呼ばれる。利用した量に応じて課金される。

③レント（ｒｅｎｔ）：一定期間の利用権を購入する。期限が過ぎれば利用できなくなる。

【００２６】前述の特願平０８－０６２０７６号の技術を用いた場合、パーチェスを実現することは容易であるが、レントを実現するのは困難である。

【００２７】ペイ・パー・ユースについては、利用する度毎にユーザが利用希望をチケット発行業者へ提出し、チケット発行業者は１回のみ使用可能なアクセスチケットを発行することにより実現することが可能であるが、頻繁にチケット発行操作が必要になる上に、１回のみ使用可能なアクセスチケットを実現するために、ユーザのＩＣカード中に使用したチケットに対するログを記録していく必要があるため、あまり現実的ではない。

【００２８】この問題に対しては、本出願人は利用制御情報をアクセスチケットの資格認証手法に導入することを提案している（特願平０８－１９１７５６号、現在未公開）。特願平０８－１９１７５６号の手法では、特願平０８－０６２０７６号に利用制御情報を導入し、情報を復号化する際に、この利用制御情報も用いるものである。利用制御情報の例としては、使用期限、使用可能回数、総使用可能時間、使用上限金額、処理の履歴を取るか否かの情報などが記載されている。

【００２９】利用制御情報が使用期限の場合には、レントを実現することが可能である。

【００３０】また利用制御情報が処理の履歴を取るという情報の場合には、一定期間後にその履歴を回収して集計することにより、利用した回数を計算し課金するという方法で、ペイ・パー・ユースに近い機能を実現することができる。さらに利用制御情報に１回あたりの利用額を記載するようにすれば、柔軟なペイ・パー・ユースを実現することが可能になる。

【００３１】つまり特願平０８－１９１７５６号の手法では、前述した権利の形態パーチェス、ペイ・パー・ユースおよびレントを全部実現できることになる。

【００３２】次に、支払の方法について考える。支払の方法としては、以下の２つが考えられる。

【００３３】①チケット発行時に支払う方法：チケット発行業者がアクセスチケットを発行する際に、支払う方法。電子貨幣により支払う場合や、発行業者側で料金を記録し、銀行振り込みなどにより清算を行う場合などがある。

【００３４】②プリペイドで支払う方法：ユーザが予めプリペイド度数を購入して、ＩＣカード中などに保持しておき、購入の際や利用の際に、プリペイドから相当する度数を引き落とす。

【００３５】特願平０８－１９１７５６号の技術を用いると、①チケット発行時に支払う方法で、前述した権利

の形態パーチェス、ペイ・パー・ユースおよびレントを全部実現できる。

【００３６】他方、②プリペイドで支払う方法では、ペイ・パー・ユースは容易に実現できる。つまり、利用制御情報に１回あたりの利用額を記載し、認証を行う度に、保持しているプリペイド情報から、利用制御情報記載の度数分ずつ引き落とせばよい。

【００３７】しかし、②プリペイドで支払う方法で、パーチェスやレントを実現するのは困難である。パーチェスは最初の利用時にのみプリペイドによる課金を行い、２回目以降の利用時には課金を行わないという処理が必要なためである。

【００３８】パーチェスに関しては、利用制御情報に利用権の買取り額を記載しておき、最初の利用時にその額を保持しているプリペイド情報から引き落として、該利用したアクセスチケットの情報をＩＣカードに登録するようにし、２回目以降の利用時には、利用しようとするチケットが既にＩＣカードに登録されているかをチェックして、登録されている時にはプリペイド情報から引き落とさないように構成することで実現することも可能ではある。しかし、この登録情報は、非常に長い期間消すことはできないので、多くのチケットを使うような場合には、ＩＣカードの記憶容量が不足することになり、あまり現実的な解決策ではない。

【００３９】レントの場合も、利用制御情報にレンタル額と有効期限を記載しておき、パーチェスと同様の方法を取ることで、実現することは可能ではあるが、同じくＩＣカードの記憶容量が不足することになり、あまり現実的な解決策ではない。

【００４０】

【発明が解決しようとする課題】本発明は、以上のような問題点に鑑みなされたものであり、プリペイドで支払う方法においても、証明データ生成装置（ＩＣカード）側に余分な負荷をかけることなく、パーチェスやレントを実現することを可能にすることを課題とする。

【００４１】

【課題を解決するための手段】本発明によれば、上述の課題を解決するために、ユーザのアクセス資格を認証するために生成され、正当性を検証される証明データを生成する証明データ生成装置に、認証用データを入力する認証用データ入力手段と、ユーザの固有情報を記憶するユーザ固有情報記憶手段と、ユーザの固有情報と、アクセス資格認証の特徴情報と、アクセス条件を記述した利用条件情報とに対し、所定の計算を実行して生成した証明用補助情報と、利用条件情報との組を含む証明用補助情報セットを記憶する証明用補助情報セット記憶手段と、入力された認証用データに対応する証明用補助情報セットを上記証明用補助情報セット記憶手段から取り出し、上記取り出した証明用補助情報セットの利用条件情報に従い、以降の処理を継続するかどうかの判断を行う利用条件判断手段と、上記利用条件判断手段において継続と判断されたときに、上記取り出した証明用補助情報セットと、上記認証用データ入力手段から入力された認証用データと、上記ユーザ固有情報記憶手段に記憶されている上記ユーザの固有情報とに所定の計算を施して証明データを生成し出力する証明データ生成出力手段とを設け、上記認証用データ入力手段から、第１の証明用補助情報セットを暗号関数における暗号化鍵で暗号化した暗号化証明用補助情報セットを入力し、上記利用条件判断手段は、上記証明用補助情報セット記憶手段から、入力された暗号化証明用補助情報セットに対応する第２の証明用補助情報セットを取り出し、上記取り出した第２の証明用補助情報セットの利用条件情報に従い、所定の処理を行った後、以降の処理を継続するかどうかの判断を行い、上記証明データ生成出力手段は、上記処理を行うことにより、上記暗号化証明用補助情報セットを復号化した結果である第１の証明用補助情報セットを出力するようにしている。

【００４２】つまり、通常の証明用補助情報セット（アクセスチケット）である第１の証明用補助情報セットを暗号化して暗号化証明用補助情報セットを作成しておき、この暗号化証明用補助情報セットへアクセスするための第２の証明用補助情報セットを用いて、通常の認証処理と全く同じ処理を行うことにより、暗号化証明用補助情報セットから、第１の証明用補助情報セットを復号化する。

【００４３】このように構成することにより、利用料金が無料のチケット（第１の証明用補助情報セット）を作成して暗号化し、暗号化されたチケットを復号化するためのチケット（第２の証明用補助情報セット）を発行し、このチケット（第２の証明用補助情報セット）の利用料金を有料としプリペイドで支払うように構成することで、全体としてプリペイドにおけるパーチェス機能の実現を可能にする。

【００４４】レント機能は、これに加えて第２の証明用補助情報セットの利用条件情報に有効期限情報を記載することで実現可能である。

【００４５】なお、暗号化されたチケットを復号化するには、通常のチケットの認証処理と同じ処理を行うように構成したので、比較的容量の少ないＩＣカード内に、余分なプログラムやデータを入れることなく、効率的に実現することが可能である。

【００４６】

【発明の実施の形態】以下、この発明の実施例について説明する。

【００４７】図１はこの実施例の構成図を示す。この実施例では、証明データ生成装置内にプリペイド情報を保持し、そのプリペイド情報を用いて、アプリケーションプログラムのアクセス権を購入する例（パーチェス）について説明する。

【００４８】図１では、証明データ生成装置で生成され出力された証明データを検証する証明データ検証装置を含めて示す。

【００４９】まず、図１に基づいて、本実施例の構成について説明したあと、証明データ検証装置、証明データ生成装置の処理の流れをフローチャートで示しながら説明する。処理の流れの説明には、通常の認証処理を例にして説明し、利用条件情報Ｌには、１回の利用の度ごとにプリペイドから引き落とされる例について説明する。そして、通常の認証処理の説明の後に、アプリケーションプログラムのアクセス権を購入する例（パーチェス）について説明する。

【００５０】［実施例の構成］図１は実施例の構成を全体として示すものであり、この図において、証明データ生成装置１０はユーザが保持するものであり、例えばＩＣカードのように内部に計算機能を持った携帯型の装置である。ＩＣカード以外にも、計算機能を持ったＰＣカードや、携帯型情報ツール、あるいはサブノートパソコンなどでもよい。内部の情報が、外部から簡単に改竄されたりすることがないように防御されていることが望ましい。

【００５１】証明データ検証装置２０はユーザがアプリケーションプログラムを使用するパソコンであり、パソコンのスロットに証明データ生成装置１０であるＩＣカードを装着して使用する。

【００５２】証明データ検証装置２０は、大きく認証用データ生成部２１と証明データ検証部２２とから構成されている。認証用データ生成部２１は、認証が必要な時に、認証用データを生成して、証明データ生成装置１０に送付する。証明データ検証部２２は、証明データ生成装置１０から送り返された証明データが正しいかどうかを検証する。

【００５３】アプリケーションプログラムは、暗号化などによりプロテクトされており、ユーザがアプリケーションプログラムを利用しようとすると、証明データ検証装置２０は、そのアプリケーションプログラムに対応した認証用データを作成し、証明データ生成装置１０に送り、証明データ生成装置１０から送り返された証明データを検証して、正しいと検証された場合に限り、アプリケーションプログラムのプロテクトを解除して、利用することを可能にする。

【００５４】一方、証明データ生成装置１０は、ユーザ固有情報記憶部１１、度数情報保持部１２、アクセスチケット記憶部１３、認証用データ入力部１４、利用条件判断部１５、証明データ生成出力部１６を含んで構成される。

【００５５】ユーザ固有情報記憶部１１は、ユーザの秘密情報を保持する部分であり、ユーザ毎に異なる情報である。ユーザ固有情報は、証明データ生成装置１０が作成された時に封入され、ユーザにも取り出せないように構成されていることが望ましい。

【００５６】度数情報保持部１２は、プリペイド情報を保持する部分であり、アプリケーションプログラムの利用や購入などに応じて、必要な額が減額されていく。額が少なくなった時には、増額することも可能である。増額の方法は、例えば、特願平９－２１３７３号で提案されている手法を用いることができる。この手法では、度数情報と署名した度数情報とを用いて度数情報を増額する。度数情報保持部１２における額の増減は、安全に行われることが必要であり、定められた方法以外でのアクセスができないように構成することが望ましい。

【００５７】アクセスチケット記憶部１３は、複数のアクセスチケットを記憶している。アクセスチケットは、ユーザにアクセス資格を与えるものであり、アプリケーションプログラム作成者、またはアプリケーションプログラム作成者から委託を受けたチケット発行業者によって作成される。本実施例では、アクセスチケットは、ユーザの固有情報と、アクセス資格認証の特徴情報と、アクセス資格認証のアクセス条件を記述した利用条件情報とに対し、所定の計算を実行して計算された証明用補助情報と利用条件情報との組である。本実施例では、アクセスチケット記憶部は、ＩＣカード中に構成されているが、アクセスチケットは発行された本人しか使えないため、コピーは自由であり、ＩＣカード外部に構成しても構わない。

【００５８】認証用データ入力部１４は、証明データ検証装置２０から送られた認証用データを入力する部分である。

【００５９】利用条件判断部１５は、入力された認証用データに対応するアクセスチケットをアクセスチケット記憶部１３から取り出し、アクセスチケット中の利用条件情報を元に、利用条件を判断する。例えば、アクセスチケットの有効期限が切れていないか、利用料金は保持しているプリペイドで支払うのに足りているか、などの利用条件を判断し、以降の処理を継続するか否かを判断する。

【００６０】証明データ生成出力部１６は、利用条件判断部１５で継続と判断された時のみ、証明データを生成して出力する。証明データは、利用条件判断部１５で取り出したアクセスチケット中の証明用補助情報と、認証用データと、ユーザの固有情報とに所定の計算を施して作成する。

【００６１】次に、具体例を挙げて、さらに詳細に説明する。ここでの説明は、通常の認証処理を例にして説明し、利用条件情報Ｌには、１回の利用の度ごとにプリペイドから引き落とされる例について説明する。

【００６２】図２は、図１の構成図に記号を付けたものである。記号は以下の説明と対応している。

【００６３】［通常の認証処理］以下では、法ｎにおけるＲＳＡ（Ｒｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｅｌｍａ

ｎ）暗号を用いた例について詳細に説明する。まず、通常の認証処理について説明する。以下の例では、アプリケーションプログラムの作成者であるソフトウェアベンダが、ＩＣカードの発行からチケットの発行まですべてを行う例について説明する。この例ではソフトウェアベンダは、すべてのユーザの秘密情報ｄｕを知っている。これ以外にも、ＩＣカードの発行とチケットとをチケット発行業者が行う構成も可能である。

【００６４】ソフトウェアベンダは、プロテクトしたいアプリケーションプログラムに対する暗号鍵を作成する。ここではＲＳＡ暗号を用いるので、大きな素数ｐ，ｑを秘密に作成し、法数ｎをｎ＝ｐ・ｑとして作成する。次に法数ｎの元で暗号鍵Ｅと復号鍵Ｄを、

【００６５】

【数１】$ED \equiv 1 \mod \phi(n)$

を満たすように生成する。ここでϕ（ｎ）はオイラー数であり、$\phi(n)=(p-1)(q-1)$である。

【００６６】次にソフトウェアベンダは、共通暗号鍵Ｋを作り、プロテクトしたいアプリケーションプログラムの一部または全部を、Ｋで暗号化し、

【００６７】

【数２】$K' = K^{F} \mod n$

を計算して、Ｋ’を暗号化したアプリケーションプログラムに、第３者が取り出せないように埋め込んで配布する。

【００６８】このアプリケーションプログラムを利用したいユーザは、予めこれに対応するアクセスチケットを入手しておくことになる。

【００６９】ソフトウェアベンダは、ユーザからのアクセスチケット発行要求を受けて、アクセスチケットを発行する。ソフトウェアベンダは、要求したユーザの秘密情報ｄｕと、アプリケーションプログラムの暗号化の際に用いた暗号鍵（Ｅ，ｎ）に対応する復号鍵（Ｄ，ｎ）とをデータベースから取り出す。次にアクセスチケットに付与する利用条件情報Ｌを作成する。ここではプリペイドから引き落として課金するので、１回の利用について引き落とす利用額をＬとする。そして、これらの情報を用いて、

【００７０】

【数３】$t = D - F(n, L, du)$

として証明用補助情報ｔを作成する。ここで関数Ｆ（）は一方向性の関数であり、一方向性ハッシュ関数ＭＤ５、ＳＨＡなどや、共通鍵暗号ＤＥＳ（ＤａｔａＥｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）などを用いることができる。

【００７１】ソフトウェアベンダは、（ｔ，Ｌ，ｎ）の組をアクセスチケットとしてユーザに発行する。

【００７２】ユーザが、アプリケーションプログラムを利用しようとすると、証明データ検証装置は、そのアプリケーションプログラムに対応した認証用データ（Ｃ，ｎ）を作成し、証明データ生成装置に送る。

【００７３】この処理の流れを図３のフローチャートに示し、これに基づいて説明する。

（ステップＳ１１）：証明データ生成部２１は、プロテクトされたアプリケーションプログラムから、Ｋ’とｎとを取り出す。

（ステップＳ１２）：証明データ生成部は、乱数ｒを生成し、乱数保持部に格納する。

（ステップＳ１３）：$C = r^{F} K' \mod n$を計算する。

（ステップＳ１４）：（Ｃ，ｎ）の組を認証用データとして証明データ生成装置１０に送付する。

【００７４】次に、証明データ生成装置１０の流れを図４に示し、これに基づいて証明データ生成装置１０の処理を説明する。

（ステップＳ２１）：認証用データ入力部１４より、認証用データ（Ｃ，ｎ）を入力する。

（ステップＳ２２）：利用条件判断部１５は、ｎをキーにしてアクセスチケット記憶部を検索し、アクセスチケット（ｔ，Ｌ，ｎ）を取り出す。

（ステップＳ２３）：利用条件判断部１５は、取り出したアクセスチケット中の利用条件Ｌ（利用額）と、度数情報保持部の度数情報Ｖとを比較する。

（ステップＳ２４～Ｓ２５）：Ｖ≧Ｌの時は、証明データ生成出力部１６は、（ステップＳ２６）に進む。そうでないときは、証明データ生成出力部は、エラーを出力して終了する。

（ステップＳ２６）：利用条件判断部１５は、度数情報保持部１２に保持されている度数情報Ｖを利用条件（利用額）Ｌの分だけ減額する。

（ステップＳ２６～Ｓ２９）：証明データ生成出力部１６は、利用条件判断部１５が取り出した証明用補助情報ｔ、利用条件Ｌ（利用額）と、ユーザ固有情報記憶部１１から読み出したｄｕとを用いて証明データＲを計算して出力する。

【００７５】

【数４】$R' = C^{F(n, L, du)} \mod n$

$R = C^{t} R' \mod n$

図４では、証明データＲを計算するのに、一旦Ｒ’の計算を分けている。これは、Ｒ’の計算にはユーザの秘密情報を用いるため、その処理が外部に漏れないように計算する必要があるが、一旦Ｒ’の計算が終われば、Ｒの計算は外部で行っても構わないためである。このようにＲ’とＲとに分けて計算してもよいし、一度に計算しても構わない。

【００７６】次に、証明データ検証装置２０の証明データ検証部の処理について説明する。証明データ生成装置１０から出力された証明データＲは、正しいユーザ固有情報ｄｕと、正しいアクセスチケット（正しい証明用補助情報ｔ、正しい利用条件Ｌ）を用いて計算されたとき

には、

【0077】

【数5】

$$R = C^{t} R' \mod n$$
$$= C^{D-F(n,L,du)} \quad C^{F(n,L,du)} \mod n$$
$$= C^{D} \mod n$$
$$= (r^{E} K')^{D} \mod n$$
$$= (r^{E} K^{E})^{D} \mod n$$
$$= (rK)^{ED} \mod n$$
$$= rK$$

となる。

【0078】そこで、証明データ検証部22では、乱数保持部23から乱数rを取り出し、

【0079】

【数6】$r^{-1} R \mod n$

を計算することで、アプリケーションを暗号化していた共通暗号鍵Kを入手することができる。証明データ検証装置は、この共通暗号鍵Kでアプリケーションの暗号化されていた部分を復号し、アプリケーションを実行することができる。

【0080】この例では、証明データ検証装置は、アプリケーションが正しく実行できたことをもって、正しく検証ができたと判断する。

【0081】以上で通常の認証処理の説明を終了する。

【0082】［パーチェス］次に、プリペイド情報を用いて、アプリケーションプログラムのアクセス権を購入する（パーチェス）例について説明する。

【0083】この機能を実現するには、通常のアクセスチケットである第1のアクセスチケットを暗号化して暗号化アクセスチケットを作成しておき、この暗号化アクセスチケットへアクセスするための第2のアクセスチケットを用いて、通常の認証処理と全く同じ処理を行うことにより、暗号化アクセスチケットから、第1のアクセスチケットを復号化する。

【0084】そしてこのとき、第1のアクセスチケットは、利用料金が無料のチケットとして作成し、第2のアクセスチケットは、利用料金を有料としプリペイドで支払うように構成することで、全体としてプリペイドにおけるパーチェス機能の実現を可能にする。

【0085】まず、パーチェスの機能を実現したいアプリケーションプログラムをＡＰ１とする。上述の説明と同様に、ＡＰ１をプロテクトする。

【0086】<アプリケーションプログラムＡＰ１のプロテクトの説明>ソフトウェアベンダは、プロテクトしたいアプリケーションプログラムに対する暗号鍵を作成する。ここではＲＳＡ暗号を用いるので、大きな素数p_1, q_1を秘密に作成し、法数n_1を$n_1 = p_1 \cdot q_1$として作成する。次に法数n_1の元で暗号鍵E_1と復号鍵D_1を、

【0087】

【数7】$E_1 \cdot D_1 \equiv 1 \mod \phi(n_1)$

を満たすように生成する。ここで$\phi(n_1)$はオイラー数であり、$\phi(n_1) = (p_1 - 1)(q_1 - 1)$である。

【0088】次にソフトウェアベンダは、共通暗号鍵K_1を作り、プロテクトしたいアプリケーションプログラムの一部または全部をK_1で暗号化し、さらに共通暗号鍵K_1を以下の式に従って、暗号鍵E_1で暗号化して、K_1'を生成する。

【0089】

【数8】$K_1' = K_1 E_1 \mod n_1$

そして、K_1'を暗号化したアプリケーションプログラムに、第3者が容易に取り出せないように埋め込んで配布する。また、n_1も、暗号化したアプリケーションプログラムに埋めこむ。

【0090】ソフトウェアベンダは、作成した（n_1, D_1, $\phi(n_1)$）の組をアクセスチケット情報データベースに記憶する。

【0091】次に、プリペイド払いパーチェス・チケットの作成について説明する。図5は、証明用補助情報生成装置30の構成例を示したものである。この例では、第1の利用条件情報と第1の復号鍵とユーザ固有情報と第2の利用条件情報とを入力として、プリペイド払いパーチェス・チケットを出力する。図5において、入力部31は、第1の利用条件情報と第1の復号鍵とユーザ固有情報と第2の利用条件情報とを入力する部分である。第1復号鍵記憶部33は、入力部31から入力された第1の復号鍵を記憶する部分である。第1の復号鍵は、アプリケーションプログラムＡＰ１の暗号化に用いた共通暗号鍵K_1を暗号化した暗号鍵（E_1, n_1）に対応する復号鍵（D_1, n_1）である。

【0092】ユーザ固有情報記憶部34は、入力部31から入力されたユーザ固有情報を記憶する部分である。これは、ユーザの証明データ生成装置10に格納されているものと同一のものである。

【0093】ユーザがチケットの発行を依頼する時には、ユーザの識別情報Ｕと、ユーザが利用を希望するアプリケーションプログラムＡＰ１から取り出したn_1とを、ソフトウェアベンダに送る。ソフトウェアベンダは、ユーザの識別情報Ｕとユーザ固有情報ｄｕとを対応づけて保持しているユーザ情報データベースから、ユーザの識別情報Ｕに対応するユーザ固有情報ｄｕを検索することによってユーザ固有情報を得、また（n, D, ϕ（n））の組を保持しているアクセスチケット情報データベースから、n_1に対応する復号鍵（D_1, n_1）を得て、証明用補助情報生成装置30に入力する。

【0094】第1利用条件情報記憶部32と第2利用条件情報記憶部35は、それぞれ第1の利用条件情報と第2の利用条件情報とを記憶する部分である。第1の利用条件情報は、アプリケーションプログラムＡＰ１の利用

条件を記述したものであり、第２の利用条件情報は、プリペイド払いパーチェス・チケットの利用条件を記述したものである。プリペイド払いパーチェス・チケットの場合には、１回目の利用時に課金され、２回目以降の利用時には課金されないという特性を持つので、第１の利用条件情報には少なくとも無料であることを意味する情報が含まれており、第２の利用条件情報には、少なくとも有料であることを意味する情報が含まれている。

【００９５】第１チケット生成部３６は、入力された第１の利用条件情報と第１の復号鍵とユーザ固有情報とに所定の計算を実行してアクセスチケットを生成する部分である。

【００９６】第１利用条件情報記憶部３２と第１復号鍵記憶部３３とユーザ固有情報記憶部３４と第１チケット生成部３６とからなる構成部分４１は、通常のアクセスチケットを生成するのと同様の構成をなしている。

【００９７】第２の鍵生成部３７は、第１チケット生成部３６で生成された第１のアクセスチケットを暗号化するための鍵を生成する部分である。

【００９８】暗号化部３８は、第１チケット生成部３６で生成された第１のアクセスチケットを、第２の鍵生成部３７で生成された暗号化鍵を用いて暗号化する部分である。

【００９９】第２チケット生成部３９は、暗号化部３８で暗号化された暗号化アクセスチケットを復号化するために必要となる第２のアクセスチケットを生成する部分である。

【０１００】チケット出力部４０は、暗号化部３８で暗号化された暗号化アクセスチケットと、第２チケット生成部３９で生成された第２のアクセスチケットとを組み合わせて、プリペイド払いパーチェス・チケットとして出力する。

【０１０１】<プリペイド払いパーチェス・チケットの作成>以下に、プリペイド払いパーチェス・チケットの作成の方法について図６のフローチャートを用いて説明する。

【０１０２】ソフトウェアベンダは、ユーザからのプリペイド払いパーチェス・チケット発行要求を受けて、プリペイド払いパーチェス・チケットを発行する。チケットの発行を依頼するユーザは、ユーザの識別情報Ｕと、ユーザが利用を希望するアプリケーションプログラムＡＰ１から取り出したn_1とを、ソフトウェアベンダに送る。

【０１０３】（ステップＳ３１）：ソフトウェアベンダは、ユーザからのプリペイド払いパーチェス・チケット発行要求であるユーザの識別情報Ｕとアプリケーションプログラム$AP1$から取り出したn_1との組（U，n_1）を入力する。また、アプリケーションプログラム$AP1$の利用条件を記述した第１の利用条件情報L_1と、プリペイド払いパーチェス・チケットの利用条件を記述した第２の利用条件情報L_2も入力する。ここでは、プリペイド払いパーチェス・チケットの生成を目的としているので、第１の利用条件情報L_1は、利用料金が無料であることを意味する

【０１０４】

【数９】$L_1=0$

であり、第２の利用条件情報Ｌ２は、パーチェスの料金が有料であることを意味する

【０１０５】

【数１０】$L_2=A$

とする。ただしＡは０以外の数字であり、たとえば１００である。

【０１０６】（ステップＳ３２）：ユーザの識別情報Ｕとユーザ固有情報ｄｕとを対応づけて保持しているユーザ情報データベースから、ユーザの識別情報Ｕに対応するユーザ固有情報ｄｕを検索する。

（ステップＳ３３）：（ｎ，Ｄ，ϕ（ｎ））の組を保持しているアクセスチケット情報データベースから、n_1に対応する第１の復号鍵（D_1，n_1）を検索する。

（ステップＳ３４）：ユーザがＡＰ１にアクセスするための第１のアクセスチケットT_1を作成する。

【０１０７】

【数１１】$T_1=(t_1, L_1, n_1)$

$t_1=D_1-F(n_1, L_1, du)$

（ステップＳ３５）：第１のアクセスチケットT_1を暗号化するために、第２の法数n_2、第２の暗号鍵E_2、第２の復号鍵D_2を生成する。大きな素数p_2，q_2を生成し、以下の式が成り立つように、法数n_2、暗号鍵E_2、復号鍵D_2を生成する。

【０１０８】

【数１２】$n_2=p_2\cdot q_2$

$E_2\cdot D_2\equiv 1 \mod \phi(n_2)$

$\phi(n_2)=(p_2-1)(q_2-1)$

（ステップＳ３６）：生成した第２の暗号鍵E_2で第１のアクセスチケットT_1を暗号化する。T_1を暗号化したものをT_1'とする。

【０１０９】

【数１３】$T_1'=T_1E_2 \mod n_2$

（ステップＳ３７）：暗号化されたアクセスチケットT_1'をユーザが復号するための第２のアクセスチケットT_2を作成する。

【０１１０】

【数１４】$T_2=(t_2, L_2, n_2)$

$t_2=D_2-F(n_2, L_2, du)$

（ステップＳ３８）：（(T_1'，n_2)，T_2）を組にしてプリペイド払いパーチェス・チケットとして出力する。

【０１１１】ソフトウェアベンダは、出力されたプリペイド払いパーチェス・チケット（(T_1'，n_2)，T_2）を、ユーザに送付する。

【０１１２】次に、プリペイド払いパーチェス・チケットの使用例について説明する。

【０１１３】＜プリペイド払いパーチェス・チケットの使用例＞

（ａ）プリペイド払いパーチェス・チケット（（T_1'，n_2），T_2）を受け取ったユーザは、まずT_2をアクセスチケット記憶部１３に格納する。

（ｂ）次に、（T_1'，n_2）を自分が保持している証明データ生成装置１０の認証用データ入力部１４より入力する。

【０１１４】以下、証明データ生成装置１０における処理が図４に従って行われる。今、証明データ生成装置１４の度数情報保持部１２には、８００度数のプリペイド情報Ｖが保持されているとする。（Ｖ＝８００）

（ステップＳ２１）：認証用データ入力部１４より、認証用データ（T_1'，n_2）を入力する。

（ステップＳ２２）：利用条件判断部１５は、n_2をキーにしてアクセスチケット記憶部１３を検索し、アクセスチケットT_2＝（t_2，L_2，n_2）を取り出す。

（ステップＳ２３）：利用条件判断部１５は、取り出したアクセスチケット中の利用条件L_2と、度数情報保持部１２の度数情報Ｖとを比較する。

（ステップＳ２４）：今、L_2＝１００、Ｖ＝８００なので、

【０１１５】

【数１５】$V \geqq L_2$

が成り立ち、（ステップＳ２６）へ進む。

（ステップＳ２６）：利用条件判断部１５は、度数情報保持部１２に保持されている度数情報Ｖを利用条件L_2の分だけ減額する。

【０１１６】

【数１６】Ｖ＝８００－１００＝７００

つまり、度数情報Ｖは、プリペイド払いパーチェス・チケットの買取り料金として、１００度数引き落とされ、残り７００度数となる。

（ステップＳ２７～Ｓ２９）：証明データ生成出力部１６は、利用条件判断部１５が取り出した証明用補助情報t_2、利用条件L_2と、ユーザ固有情報記憶部１１から読み出したｄｕとを用いて証明データＲを計算して出力する。

【０１１７】

【数１７】$R' = T_1'^{F(n2, L2, du)} \mod n_2$

$R = T_1'^{t2} R' \mod n_2$

Ｒの計算を行うと、

【０１１８】

【数１８】

$R = T_1'^{t2} R' \mod n_2$

$= T_1'^{D2-F(n2, L2, du)} C^{F(n2, L2, du)} \mod n_2$

$= T_1'^{D2} \mod n_2$

$= (T_1^{E2})^{D2} \mod n_2$

$= T_1$

という計算が成り立ち、証明データ生成出力部１６から、証明データＲとして

【０１１９】

【数１９】$R = T_1$

が出力される。

【０１２０】つまり、（T_1'，n_2）を自分が保持している証明データ生成装置１０の認証用データ入力部１４より入力すると、L_2が度数情報Ｖから引き落とされて、結果としてT_1'が復号されたT_1が出力される。

【０１２１】（ｃ）ユーザは、入手したT_1をアクセスチケット記憶部１３に格納する。

【０１２２】（ｄ）ユーザは、アプリケーションプログラムＡＰ１を利用するためのアクセスチケットT_1を入手できたので、アプリケーションプログラムＡＰ１を利用する。

【０１２３】以下、証明データ検証装置１０における認証用データ生成処理が図３に従って行われる。

（ステップＳ１１）：認証用データ生成部２１は、プロテクトされたアプリケーションプログラムから、K_1'とn_1とを取り出す。

（ステップＳ１２）：認証用データ生成部２１は、乱数ｒを生成し、乱数保持部２３に格納する。

（ステップＳ１３）：$C = r^E K_1' \mod n_1$を計算する。

（ステップＳ１４）：（Ｃ，n_1）の組を認証用データとして証明データ生成装置１０に送付する。

（ｅ）証明データ生成装置１０における処理が再び図４に従って行われる。

（ステップＳ２１）：認証用データ入力部１４より、認証用データ（Ｃ，n_1）を入力する。

（ステップＳ２２）：利用条件判断部１５は、n_1をキーにしてアクセスチケット記憶部１３を検索し、アクセスチケットT_1＝（t_1，L_1，n_1）を取り出す。

（ステップＳ２３）：利用条件判断部１５は、取り出したアクセスチケット中の利用条件L_1と、度数情報保持部１２の度数情報Ｖとを比較する。

（ステップＳ２４）：今、Ｌ１＝０、Ｖ＝７００なので、

【０１２４】

【数２０】$V \geqq L_1$

が成り立ち、（ステップＳ２６）へ進む。

（ステップＳ２６）：利用条件判断部１５は、度数情報保持部１２に保持されている度数情報Ｖを利用条件L_1の分だけ減額する。

【０１２５】

【数２１】Ｖ＝７００－０＝７００

つまり、度数情報Ｖは、最初にプリペイド払いパーチェス・チケットの買取り料金として、１００度数引き落とされているので、２回目以降の利用では引き落とされ

ず、残り７００度数のままとなる。

（ステップＳ２７～Ｓ２９）：証明データ生成出力部１６は、利用条件判断部１５が取り出した証明用補助情報t_i、利用条件L_iと、ユーザ固有情報記憶部１１から読み出したｄｕとを用いて証明データＲを計算して出力する。

【０１２６】

【数２２】$R' = C^{F(n, L_i, du)} \mod n_i$

$R = C^{t_i} R' \mod n_i$

つまり、

【０１２７】

【数２３】

$R = C^{t_i} R' \mod n_i$

$= r^k$

（ｆ）証明データ検証装置２０の証明データ検証部２２は通常の認証と同様に処理を行い、乱数保持部２３から乱数ｒを取り出し、

【０１２８】

【数２４】$r^{-1} R \mod n_i$

を計算することで、アプリケーションを暗号化していた共通暗号鍵Ｋを入手することができる。証明データ検証装置は、この共通暗号鍵Ｋでアプリケーションの暗号化されていた部分を復号し、アプリケーションを実行することができる。

【０１２９】これ以降は、何度アプリケーションプログラムＡＰ１を実行しても、同様の処理が行われ、無料で利用することができる。

【０１３０】以上説明したように、上記のように構成することで、プリペイド情報を用いて、アプリケーションプログラムのアクセス権を購入する（パーチェス）ことが可能になる。

【０１３１】以上、プリペイドにおけるパーチェス機能の実現について説明した。

【０１３２】これ以外にも、証明データ生成装置に時計を備え、第１のアクセスチケットの利用条件情報Ｌの中に、利用額が無料という情報に加えて、有効期限情報を記載し、第１のアクセスチケットの利用のたびに、時刻と比較することによって、プリペイドにおけるレント機能を実現することも可能である。

【０１３３】さらに、別の例としては、証明データ生成装置に時計を備え、第２のアクセスチケットの利用条件情報Ｌの中に、有効期限情報を記載し、暗号化された第１のアクセスチケットの復号の際に、時刻と比較することによって、第１のアクセスチケットを配布（解凍）する期限を限定することなども可能である。

【０１３４】また、本実施例では、ＲＳＡ暗号を元にして説明を行ったが、これに限らず他の暗号方式を用いても構わない。また、アクセスチケットの実現式もこれに限ることはない。

【０１３５】

【発明の効果】実行制御等のユーザのアクセス資格の認証を行うに際して、ユーザはあらかじめ固有情報を保持し、プログラム作成者等のプロテクト者はユーザが所持する固有情報とは独立にアクセス資格認証の特徴情報を用意し、アクセスチケットをユーザの固有情報とアプリケーションプログラムの作成等に使用したアクセス資格認証の特徴情報とに応じて作成し、配布することにより、ユーザおよびプロテクト者の双方を、アクセス権情報管理のわずらわしさから開放させるという特徴を残したまま、従来は困難だったプリペイドにおけるパーチェス機能およびレント機能を実現することを可能にした。

【０１３６】さらにこれらの機能を実現するにおいて、通常のチケットの認証処理と同じ処理を行うように構成したので、比較的容量の少ないＩＣカード内に、余分なプログラムやデータを入れることなく、効率的に実現することが可能である。

【図面の簡単な説明】

【図１】　本発明の実施例の構成を示すブロック図である。

【図２】　図１の構成を詳細に説明する図である。

【図３】　図１の証明データ検証装置の認証用データ生成処理を説明するフローチャートである。

【図４】　図１の証明データ生成装置の証明データ生成処理を説明するフローチャートである。

【図５】　図１の証明データの生成に用いるチケットを生成する証明用補助情報生成装置を示すブロック図である。

【図６】　図１の証明データの生成に用いるチケットの生成を説明する図である。

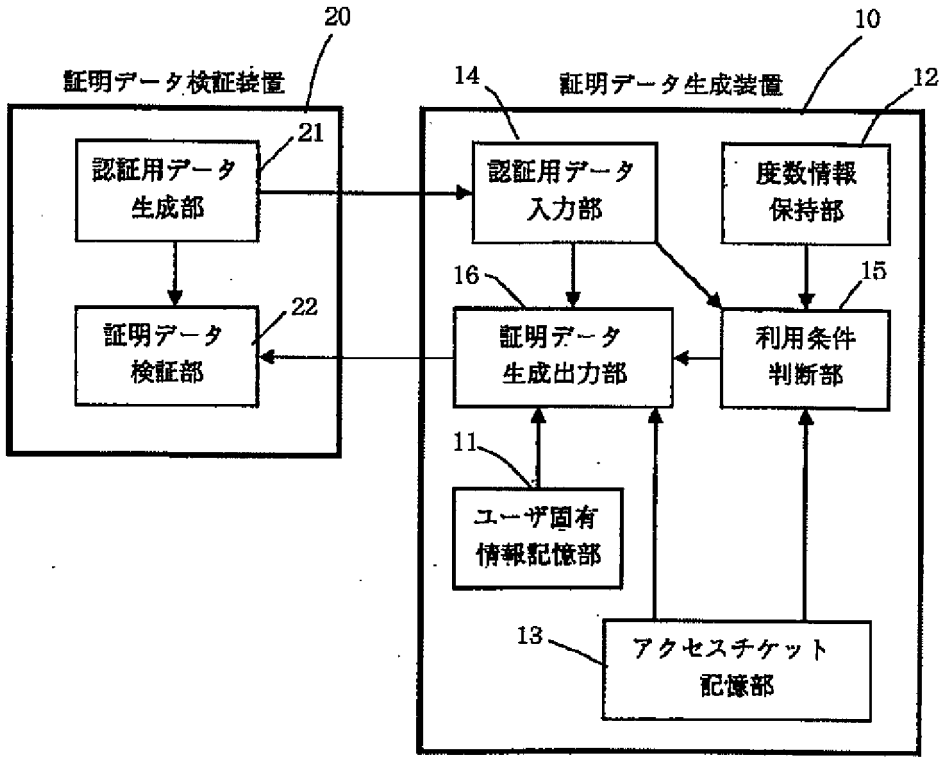
【符号の説明】

１０　証明データ生成装置
１１　ユーザ固有情報記憶部
１２　度数情報保持部
１３　アクセスチケット記憶部
１４　認証用データ入力部
１５　利用条件判断部
１６　証明データ生成出力部
２０　証明データ検証装置
２１　認証用データ生成部
２２　証明データ検証部
２３　乱数保持部
３０　証明用補助情報生成装置
３２　第１利用条件情報記憶部
３３　第１復号鍵記憶部
３４　ユーザ固有情報記憶部
３５　第２利用条件記憶部
３６　第１チケット生成部
３７　第２の鍵生成部
３８　暗号化部
３９　第２チケット生成部

23　　24

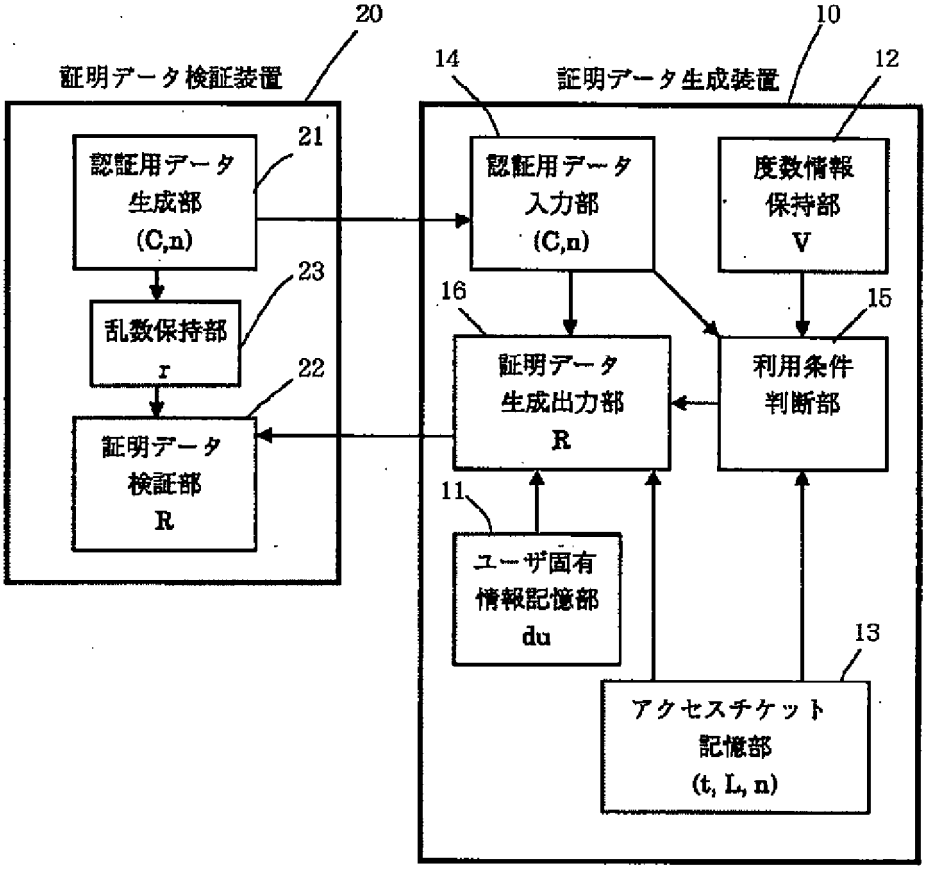
４０　チケット出力部

【図１】



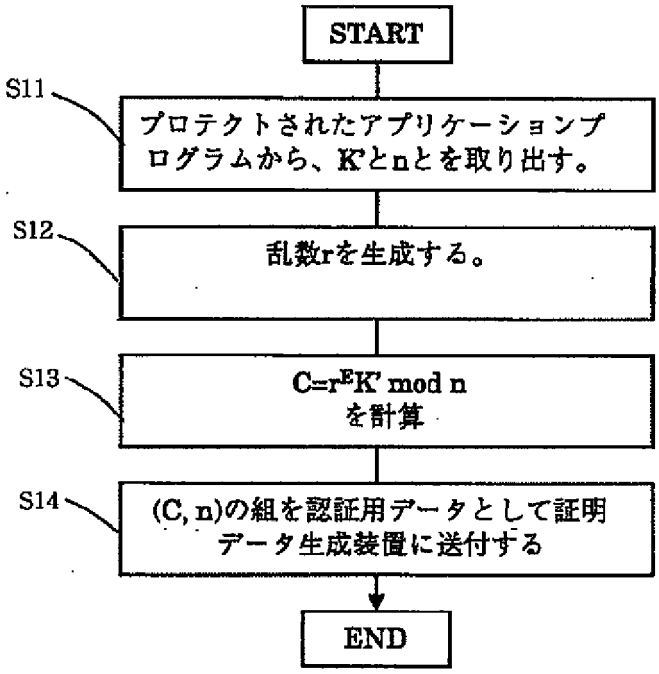
実施例の構成図

【図２】



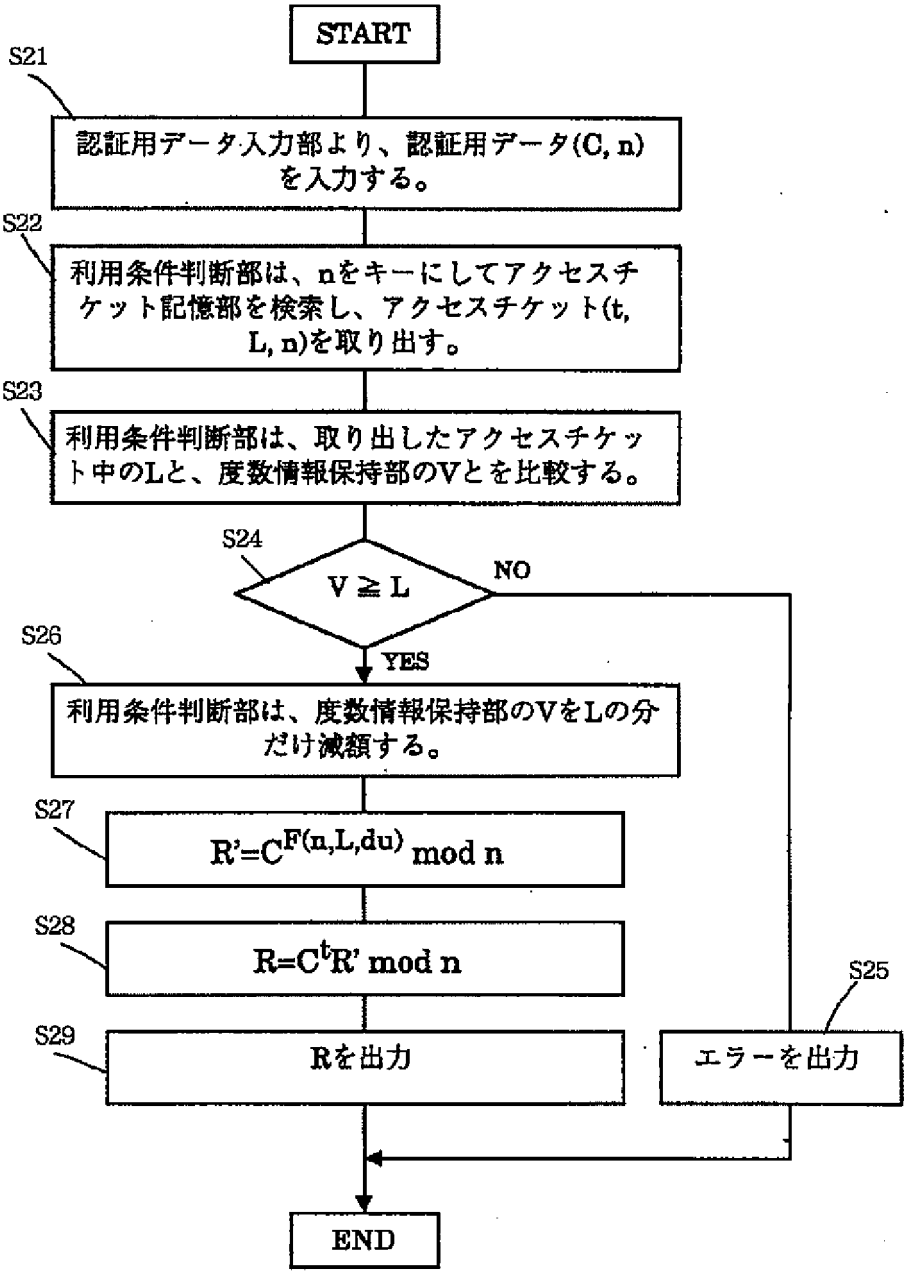
実施例の詳細構成図

【図３】



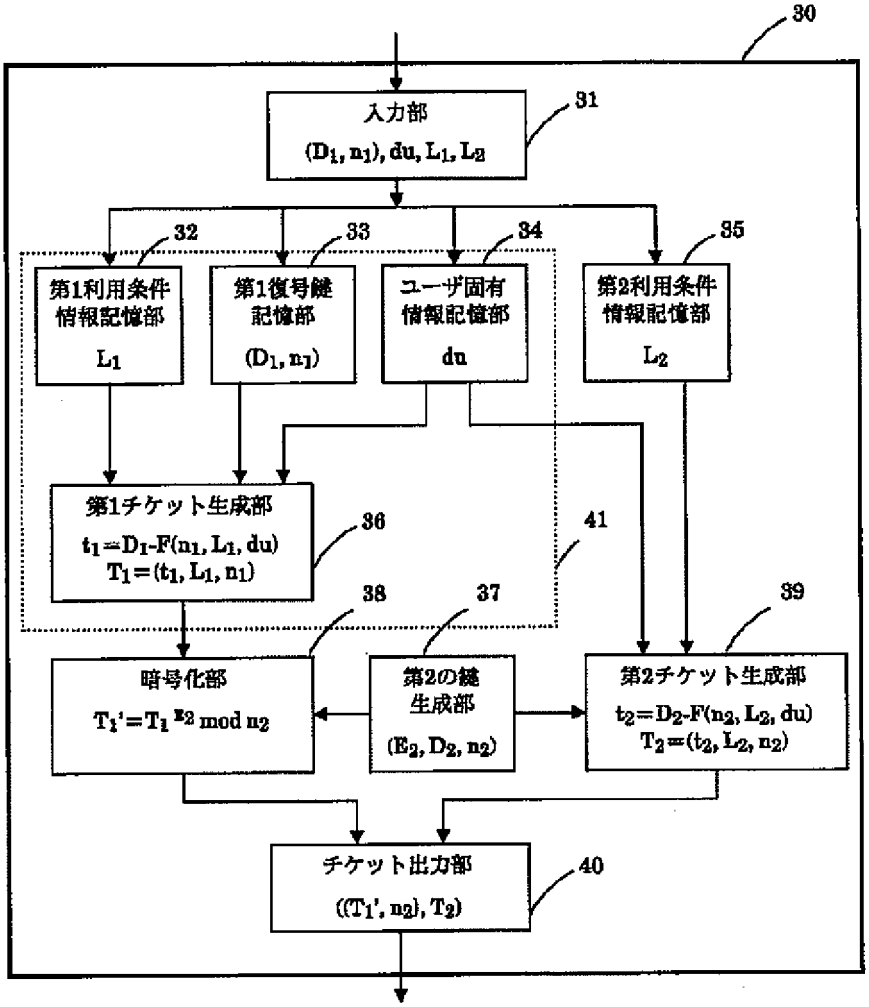
証明データ検証装置における認証用データ生成処理

【図４】



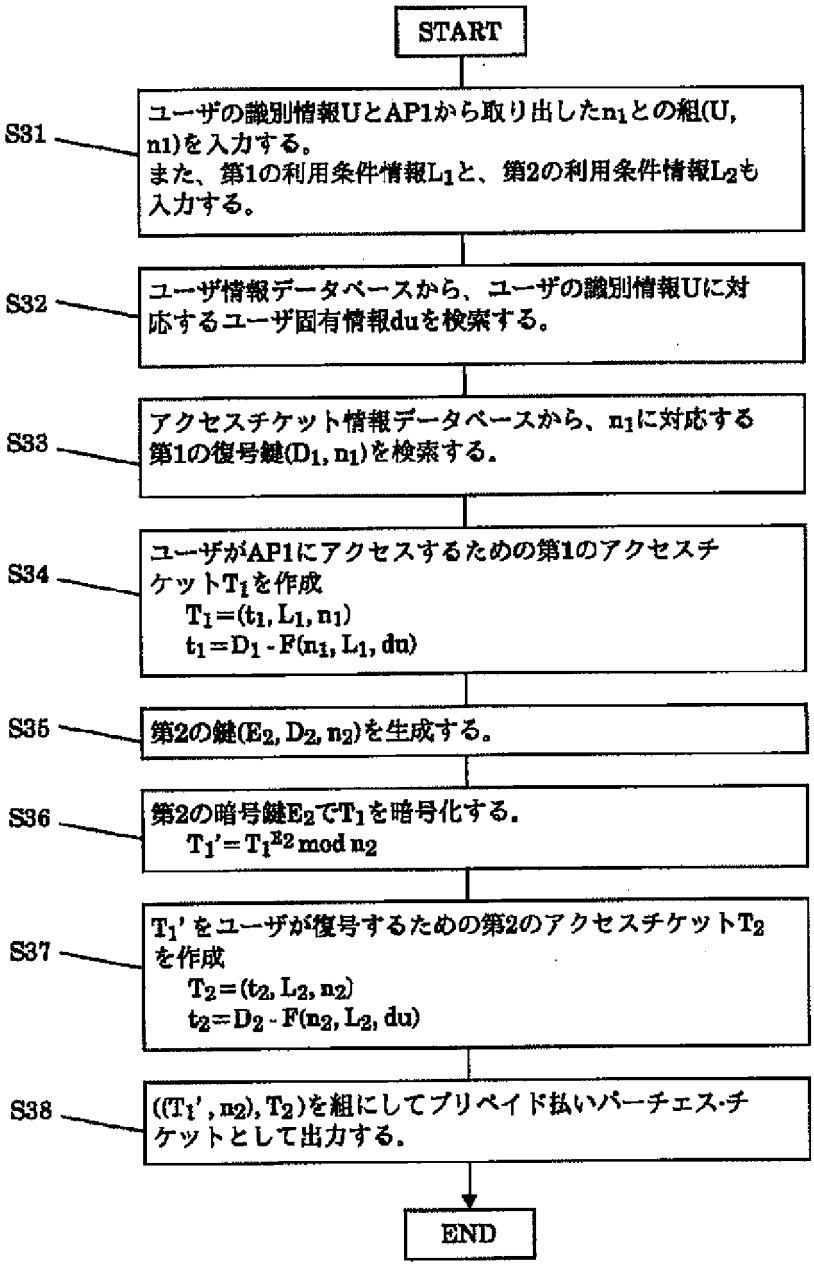
証明データ生成装置における処理

【図５】



証明用補助情報生成装置の構成図

【図６】



プリペイド払いパーチェスチケット作成処理